S03P1010 US00

# 日　本　国　特　許　庁
## JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００２年　８月２８日

出願番号
Application Number: 特願２００２－２４９２６３

[ST.10/C]: [ＪＰ２００２－２４９２６３]

出願人
Applicant(s): ソニー株式会社

２００３年　６月１０日

特許庁長官
Commissioner,
Japan Patent Office 太田信一郎

出証番号　出証特２００３－３０４４９４３

【書類名】　特許願
【整理番号】　0290574607
【提出日】　平成14年 8月28日
【あて先】　特許庁長官　殿
【国際特許分類】　H04L　9/00
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　筒井　京弥
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　羽田　直也
【特許出願人】
　【識別番号】　000002185
　【氏名又は名称】　ソニー株式会社
【代理人】
　【識別番号】　100067736
　【弁理士】
　【氏名又は名称】　小池　晃
【選任した代理人】
　【識別番号】　100086335
　【弁理士】
　【氏名又は名称】　田村　榮一
【選任した代理人】
　【識別番号】　100096677
　【弁理士】
　【氏名又は名称】　伊賀　誠司

【手数料の表示】

【予納台帳番号】　019530

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9707387

【プルーフの要否】　要

【書類名】明細書

【発明の名称】　符号列暗号化方法、装置および暗号解除方法、装置および記録媒体

【特許請求の範囲】

【請求項１】　信号を符号化して得られた符号列（「原符号列」という）の少なくとも一部のフレームの符号列から、再生品質が低い符号列を含む第一の符号列と、上記第一の符号列の再生信号の高品質化に用いる第二の符号列と、を生成する生成工程と、

上記第二の符号列を暗号化する暗号化工程と、

を含み、

上記暗号化工程では、

上記第二の符号列において完全にまたは殆ど規則的な値をとる第一の部分は、第一の暗号化処理で暗号化され、もしくは暗号化されず、

上記第二の符号列において上記第一の部分以外の少なくとも一部（「第二の部分」という）は、上記第一の暗号化処理とは異なる第二の暗号化処理で暗号化される、

ことを特徴とする符号列生成方法。

【請求項２】　上記第二の符号列の上記第一の部分は、再生帯域情報または同期信号情報の少なくとも一つを含む

ことを特徴とする請求項1記載の符号列生成方法。

【請求項３】　上記第一の部分の少なくとも一部は、上記第一の符号列の内、上記第一の符号列の試聴再生時に無視される部分に埋め込まれる、ことを特徴とする請求項1記載の符号列生成方法。

【請求項４】　上記生成工程は、上記原符号列の少なくとも一部をダミーデータで置換する置換工程を含み、

上記第一の符号列は、上記原符号列の置換されていない部分および上記ダミーデータを含み、

上記第二の符号列は、上記ダミーデータで置換された上記原符号列の真のデータの少なくとも一部を含む、

ことを特徴とする、請求項1記載の符号列生成方法。

【請求項５】　上記ダミーデータで置換された上記原符号列の真のデータの少なくとも他の一部は、上記第一の符号列の上記ダミーデータとは異なる部分に含まれる

ことを特徴とする、請求項4記載の符号列生成方法。

【請求項６】　信号を符号化して得られた符号列の少なくとも一部のフレームの符号列から、再生品質が低い符号列を含む第一の符号列と、上記第一の符号列の再生信号の高品質化に用いる第二の符号列と、を生成する生成手段と、

上記第二の符号列を暗号化する暗号化手段と、

を備え、

上記暗号化手段では、

上記第二の符号列において完全にまたは殆ど規則的な値をとる第一の部分は、第一の暗号化処理で暗号化され、もしくは暗号化されず、

上記第二の符号列において上記第一の部分以外の少なくとも一部（「第二の部分」という）は、上記第一の暗号化処理とは異なる第二の暗号化処理で暗号化される、

ことを特徴とする符号列生成装置。

【請求項７】　上記第二の符号列の第一の部分は、再生帯域情報または同期信号情報の少なくとも一つを含む

ことを特徴とする請求項6記載の符号列生成装置。

【請求項８】　上記第一の部分は、上記第一の符号列の内、上記第一の符号列の試聴再生時に無視される部分に埋め込まれる、ことを特徴とする請求項6記載の符号列生成装置。

【請求項９】　上記生成手段は、上記原符号列の少なくとも一部をダミーデータで置換する置換手段を含み、

上記第一の符号列は、上記原符号列の置換されていない部分および上記ダミーデータを含み、

上記第二の符号列は、上記ダミーデータで置換された上記原符号列の真のデータの少なくとも一部を含む、

ことを特徴とする、請求項6記載の符号列生成装置。

【請求項１０】　上記ダミーデータで置換された上記原符号列の真のデータの少なくとも他の一部は、上記第一の符号列の上記ダミーデータとは異なる部分に含まれる

ことを特徴とする、請求項9記載の符号列生成装置。

【請求項１１】　暗号化された符号列の暗号解除方法であって：

暗号化前の符号列において暗号化前に完全にまたは殆ど規則的な値をとっていた第一の部分に対応する第一の暗号列を、第一の解除処理で暗号解除するまたは暗号解除しない第一の暗号解除工程と、

暗号化前の符号列において上記第一の部分以外の少なくとも一部（「第二の部分」という）に対応する第二の暗号列を、第一の解除方法とは異なる第二の暗号解除処理で暗号解除する第二の暗号解除工程と、

を含むことを特徴とする暗号解除方法。

【請求項１２】　上記暗号化された符号列は、再生品質が低い符号列を含む他の符号列の再生時に、その再生信号の高品質化に用いられるものであり、

上記暗号化された符号列と上記他の符号列は、信号を符号化して得られた原符号列の少なくとも一部のフレームの符号列に所定の処理を施すことにより生成されるものである、

ことを特徴とする、請求項11記載の暗号解除方法。

【請求項１３】　上記第一の部分は、再生帯域情報または同期信号情報を含む

ことを特徴とする請求項11記載の暗号解除方法。

【請求項１４】　上記第一の部分は、上記他の符号列の内、上記第一の符号列の試聴再生時に無視される部分に埋め込まれたものである、ことを特徴とする請求項11記載の暗号解除方法。

【請求項１５】　第１および第2の暗号解除工程の前に、上記第１の暗号列と上記第２の暗号列とを所定の方法で並べ直す並べ直し工程を、

さらに含むことを特徴とする請求項11記載の暗号解除方法。

【請求項１６】　暗号化された符号列の暗号解除装置であって：

暗号化前の符号列において暗号化前に完全にまたは殆ど規則的な値をとってい

た第一の部分に対応する第一の暗号列を、第一の解除処理で暗号解除するまたは暗号解除しない第一の暗号解除手段と、

暗号化前の符号列において上記第一の部分以外の少なくとも一部（「第二の部分」という）に対応する第二の暗号列を、第一の解除方法とは異なる第二の暗号解除処理で暗号解除する第二の暗号解除手段と、

を含むことを特徴とする暗号解除装置。

【請求項１７】　上記暗号化された符号列は、再生品質が低い符号列を含む他の符号列の再生時に、その再生信号の高品質化に用いられるものであり、

上記暗号化された符号列と上記他の符号列は、信号を符号化して得られた原符号列の少なくとも一部のフレームの符号列に所定の処理を施すことにより生成されるものである、

ことを特徴とする、請求項16記載の暗号解除装置。

【請求項１８】　上記第一の部分は、再生帯域情報または同期信号情報の少なくとも一つを含む

ことを特徴とする請求項16記載の暗号解除装置。

【請求項１９】　上記第一の部分は、上記他の符号列の内、上記第一の符号列の試聴再生時に無視される部分に埋め込まれたものである、ことを特徴とする請求項16記載の暗号解除装置。

【請求項２０】　第１および第2の暗号解除手段には、上記第１の暗号列と上記第２の暗号列とを所定の方法で並べ直してから暗号化された符号列の入力が行われる、

ことを特徴とする請求項16記載の暗号解除装置。

【請求項２１】　符号列を暗号化する方法において、上記符号列を完全に、または殆ど規則的な値をとる第一の符号列部分と、その他の部分からなる第二の符号列部分に分離し、上記第一の符号列部分は第一の方法で暗号化するか、もしくは全く暗号化せず、上記第二の符号列部分は上記第一の方法とは別の方法で暗号化することを特徴とする符号列暗号化方法。

【請求項２２】　符号列を暗号化する手段において、上記符号列を完全に、または殆ど規則的な値をとる第一の符号列部分と、その他の部分からなる第二の符

号列部分に分離し、上記第一の符号列部分は第一の方法で暗号化するか、もしくは全く暗号化せず、上記第二の符号列部分は上記第一の方法とは別の方法で暗号化することを特徴とする符号列暗号化装置。

【請求項２３】　第一の方法で暗号化されたか、あるいは、全く暗号化されていない、完全に、または殆ど規則的な値をとる第一の符号列部分と、第二の方法で暗号化されたその他の部分からなる第二の符号列部分が記録されていることを特徴とする記録媒体。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】

本発明は、試し視聴が可能なように信号を符号化するとともに、その結果、試し視聴者が購入を決めれば、少ない情報量のデータを追加して高品質での再生や記録を可能にする方法に関するものである。

【０００２】

【従来の技術】

例えば音響などの信号を暗号化して放送したり、記録媒体に記録して、鍵を購入した者に対してのみ、その視聴を許可するというソフトの流通方法が知られている。暗号化の方法としては、例えば、PCMの音響信号のビット列に対して鍵信号として乱数系列の初期値を与え、発生した0/1の乱数系列と上記PCMのビット列との排他的論理和をとったビット列を送信したり記録媒体に記録する方法が知られている。この方法を使用することにより、鍵信号を入手した者のみがその音響信号を正しく再生できるようにし、鍵信号を入手しなかった者は雑音しか再生できないようにすることができる。もちろん、暗号化方法としては、より複雑な方法を用いることも可能であり、例えば、所謂DES等を利用するようにしてもよい。

【０００３】

DESに関しては例えば、

[0]

Federal Information Processing Standards Publication 46

Specifications for the DATA ENCRYPTION STANDARD

1977, January 15

にその規格の内容が述べられている。

【０００４】

一方、音響信号を圧縮して放送したり、記録媒体に記録する方法が、普及しており、符号化されたオーディオ或いは音声等の信号を記録可能な光磁気ディスク等の記録媒体が広く使用されている。オーディオ或いは音声等の信号の高能率符号化の手法には種々あるが、例えば、時間軸上のオーディオ信号等をブロック化しないで、複数の周波数帯域に分割して符号化する非ブロック化周波数帯域分割方式である、帯域分割符号化(サブ・バンド・コーディング：SBC)や、時間軸の信号を周波数軸上の信号に変換(スペクトル変換)して複数の周波数帯域に分割し、各帯域毎に符号化するブロック化周波数帯域分割方式、いわゆる変換符号化等を挙げることができる。また、上述の帯域分割符号化と変換符号化とを組み合わせた高能率符号化の手法も考えられており、この場合には、例えば、上記帯域分割符号化で帯域分割を行った後、該各帯域毎の信号を周波数軸上の信号にスペクトル変換し、このスペクトル変換された各帯域毎に符号化が施される。

【０００５】

ここで上述したフィルターとしては、例えばQMFフィルターがあり、

[1]

1976 R.E.Crochiere Digital coding of speech in subbands

Bell Syst.Tech. J. Vol.55,No.8 1976

に述べられている。

【０００６】

また

[2]

ICASSP 83,BOSTON Polyphase Quadrature filters-A new subband coding techn ique

Joseph H. Rothweiler

には等バンド幅のフィルター分割手法が述べられている。

【０００７】

ここで、上述したスペクトル変換としては、例えば、入力オーディオ信号を所定単位時間(フレーム)でブロック化し、当該ブロック毎に離散フーリエ変換(DFT)、コサイン変換(DCT)、モディファイドDCT変換(MDCT)等を行うことで時間軸を周波数軸に変換するようなスペクトル変換がある。

【０００８】

MDCTについては

[3]

ICASSP 1987

Subband/Transform Coding

Using Filter Bank Designs Based on Time Domain Aliasing Cancellation

J.P.Princen A.B.Bradley Univ. of Surrey Royal Melbourne Inst.of Tech

.

に述べられている。

【０００９】

波形信号をスペクトルに変換する方法として上述のDFTやDCTを使用した場合には、M個のサンプルからなる時間ブロックで変換を行うとM個の独立な実数データが得られる。時間ブロック間の接続歪みを軽減するために通常、両隣のブロックとそれぞれM1個のサンプルずつオーバーラップさせるので、平均して、DFTやDCTでは(M-M1)個のサンプルに対してM個の実数データを量子化して符号化することになる。

【００１０】

これに対してスペクトルに変換する方法として上述のMDCTを使用した場合には、両隣の時間とM個ずつオーバーラップさせた2M個のサンプルから、独立なM個の実数データが得られるので平均して、MDCTではM個のサンプルに対してM個の実数データを量子化して符号化することになる。復号装置においては、このようにしてMDCTを用いて得られた符号から各ブロックにおいて逆変換を施して得られた波形要素を互いに干渉させながら加え合わせることにより、波形信号を再構成することができる。

【００１１】

一般に変換のための時間ブロックを長くすることによって、スペクトルの周波数分解能が高まり特定のスペクトル成分にエネルギーが集中する。したがって、両隣のブロックと半分ずつオーバーラップさせて長いブロック長で変換を行い、しかも得られたスペクトル信号の個数が、元の時間サンプルの個数に対して増加しないMDCTを使用することにより、DFTやDCTを使用した場合よりも効率の良い符号化を行うことが可能となる。また、隣接するブロック同士に十分長いオーバーラップを持たせることによって、波形信号のブロック間歪みを軽減することもできる。

【００１２】

このようにフィルターやスペクトル変換によって帯域毎に分割された信号を量子化することにより、量子化雑音が発生する帯域を制御することができ、マスキング効果などの性質を利用して聴覚的により高能率な符号化を行なうことができる。また、ここで量子化を行なう前に、各帯域毎に、例えばその帯域における信号成分の絶対値の最大値で正規化を行なうようにすれば、さらに高能率な符号化を行なうことができる。

【００１３】

周波数帯域分割された各周波数成分を量子化する周波数分割幅としては、例えば人間の聴覚特性を考慮した帯域分割が行われる。すなわち、一般に臨界帯域(クリティカルバンド)と呼ばれている高域程帯域幅が広くなるような帯域幅で、オーディオ信号を複数(例えば２５バント)の帯域に分割することがある。また、この時の各帯域毎のデータを符号化する際には、各帯域毎に所定のビット配分或いは、各帯域毎に適応的なビット割当て(ビットアロケーション)による符号化が行われる。例えば、上記MDCT処理されて得られた係数データを上記ビットアロケーションによって符号化する際には、上記各ブロック毎のMDCT処理により得られる各帯域毎のMDCT係数データに対して、適応的な割当てビット数で符号化が行われることになる。

【００１４】

ビット割当手法としては、次の２手法が知られている。

【００１５】

[4]

Adaptive Transform Coding of Speech Signals

R.Zelinski and P.Noll

IEEE Transactions of Accoustics,Speech,and Signal Processing,

vol.ASSP-25,No.4,August 1977

では、各帯域毎の信号の大きさをもとに、ビット割当を行なっている。この方式では、量子化雑音スペクトルが平坦となり、雑音エネルギー最小となるが、聴感覚的にはマスキング効果が利用されていないために実際の雑音感は最適ではない。また

【００１６】

[5]

ICASSP 1980

The critical band coder

--digital encoding of the perceptual requirements of the auditory system

M.A.Kransner MIT

では、聴覚マスキングを利用することで、各帯域毎に必要な信号対雑音比を得て固定的なビット割当を行なう手法が述べられている。しかしこの手法ではサイン波入力で特性を測定する場合でも、ビット割当が固定的であるために特性値が、それほど良い値とならない。

【００１７】

これらの問題を解決するために、ビット割当に使用できる全ビットが、各小ブロック毎にあらかじめ定められた固定ビット割当パターン分と、各ブロックの信号の大きさに依存したビット配分を行なう分に分割使用され、その分割比を入力信号に関係する信号に依存させ、前記信号のスペクトルが滑らかなほど前記固定ビット割当パターン分への分割比率を大きくする高能率符号化装置が提案されている。

【００１８】

この方法によれば、サイン波入力のように、特定のスペクトルにエネルギーが集中する場合にはそのスペクトルを含むブロックに多くのビットを割り当てる事により、全体の信号対雑音特性を著しく改善することができる。一般に、急峻なスペクトル成分をもつ信号に対して人間の聴覚は極めて敏感であるため、このような方法を用いる事により、信号対雑音特性を改善することは、単に測定上の数値を向上させるばかりでなく、聴感上、音質を改善するのに有効である。

【００１９】

ビット割り当ての方法にはこの他にも数多くのやり方が提案されており、さらに聴覚に関するモデルが精緻化され、符号化装置の能力があがれば聴覚的にみてより高能率な符号化が可能になる。これらの方法においては、計算によって求められた信号対雑音特性をなるべく忠実に実現するような実数のビット割り当て基準値を求め、それを近似する整数値を割り当てビット数とすることが一般的である。

【００２０】

また本発明人らによる発明、国際公開番号WO94/28633(対応米国特許番号US5717821)では、スペクトル信号から聴感上特に重要なトーン性の成分、すなわち特定の周波数周辺にエネルギーが集中している信号成分、を分離して、他のスペクトル成分とは別に符号化する方法が提案されており、これにより、オーディオ信号等を聴感上の劣化を殆ど生じさせずに高い圧縮率で効率的に符号化することが可能になっている。

【００２１】

実際の符号列を構成するにあたっては、先ず、正規化および量子化が行なわれる帯域毎に量子化精度情報、正規化係数情報を所定のビット数で符号化し、次に、正規化および量子化されたスペクトル信号を符号化すれば良い。

【００２２】

また、

ISO/IEC 11172-3: 1993(E), 1993

では、帯域によって量子化精度情報を表すビット数が異なるように設定された高能率符号化方式が記述されており、高域になるにしたがって、量子化精度情報を

表すビット数が小さくなるように規格化されている。

【００２３】

量子化精度情報を直接符号化するかわりに、復号装置において、例えば、正規化係数情報から量子化精度情報を決定する方法も知られているが、この方法では、規格を設定した時点で正規化係数情報と量子化精度情報の関係が決まってしまうので、将来的にさらに高度な聴覚モデルに基づいた量子化精度の制御を導入することができなくなる。また、実現する圧縮率に幅がある場合には圧縮率毎に正規化係数情報と量子化精度情報との関係を定める必要が出てくる。

【００２４】

量子化されたスペクトル信号を、例えば、

D.A.Huffman: A Method for Construction of Minimum Redundancy Codes, Proc.I.R.E., 40, p.1098 (1952)

に述べられている可変長符号を用いて符号化することによって、より効率的に符号化する方法も知られている。

【００２５】

上述のように符号化された信号をPCM信号の場合と同様に暗号化して配布することも可能で、この場合、鍵信号を入手していない者は元の信号を再生することはできない。また、符号化されたビット列を暗号化するのではなく、PCM信号をランダム信号に変換した後、圧縮のための符号化を行なう方法もあり、この場合も鍵信号を入手していない者は雑音しか再生することはできない。

【００２６】

しかしながら、これらのスクランブル方法では、鍵が無い場合、あるいは通常の再生手段で再生させた場合には、それを再生させると雑音になってしまい、そのソフトの内容把握をすることはできない。このため、例えば、比較的低音質で音楽を記録したディスクを配布し、それを試聴した者が自分の気に入ったものに対してだけ鍵を購入して高音質で再生できるようにする、あるいはそのソフトを試聴してから高音質で記録されたディスクを新たに購入できるようにする、といった用途に利用することができなかった。

【００２７】

また従来、高能率符号化を施した信号を暗号化する場合に、通常の再生手段にとって意味のある符号列を与えながら、その圧縮効率を下げないようにすることは困難であった。すなわち、前述のように、高能率符号を施してできた符号列にスクランブルをかけた場合、その符号列を再生しても雑音が発生するばかりではなく、スクランブルによってできた符号列が、元の高能率符号の規格に適合していない場合には、再生手段がまったく動作しないこともありうる。また逆に、PCM信号にスクランブルをかけた後、高能率符号化した場合には例えば聴覚の性質を利用して情報量を削っていると、その高能率符号化を解除した時点で、必ずしも、PCM信号にスクランブルをかけた信号が再現できるわけでは無いので、スクランブルを正しく解除することは困難なものになってしまう。このため、圧縮の方法としては効率は下がっても、スクランブルが正しく解除できる方法を選択する必要があった。

【００２８】

これに対して、本発明人等による、特開平10-135944号公報によれば、例えば音楽信号をスペクトル信号に変換して符号化したもののうち、高域側のみを暗号化して狭帯域の信号であれば、鍵が無くても試聴が可能なオーディオ符号化方式が開示されている。即ち、この方式では例えば、高域側を暗号化するとともに、高域側のビット割り当て情報等をダミーデータに置き換え、高域側の真のビット割り当て情報は、通常のデコーダが無視する位置に記録している。この方式を採用すれば、例えば、試聴の結果、気に入った音楽だけを高音質で楽しむことが可能となる。

【００２９】

しかしながら、特開平10-135944号公報による方法では、その安全性を暗号化のみに依存しているため、万一、暗号が解読された場合には、料金を徴収できないまま、高音質の音楽を聴くことができてしまう可能性がある。

【００３０】

これを解決する方法として、国際出願番号PCT/JP02/01106では、記録媒体に記録する一部の情報をダミーデータとして記録して比較的低い品質で再生できるようにしておき、高品質再生が必要になった時に、そのダミーデータを真のデータ

に記録仕直すことにより、暗号が解読される可能性をなくすと共に、低品質、高品質のどちらのフォーマットで記録された媒体でも通常の再生装置で視聴可能にする方法が提案されている。この方法を用いれば、暗号鍵を利用する方法と比較して、安全性を高めながら、コンテンツの内容を確認してから、その高品質化を行なうことができるようになった。

【００３１】

しかしながら、国際出願番号PCT/JP02/01106(本件出願時未公開)の方法では、高品質化を行なうためにダミーデータを書き換える必要があり、そのデータ量は試し視聴用ファイルに比較すれば小さいが、まだ大きいため、それを送信する通信時間が比較的長くかかり、結果的に高品質化のための時間が長くかかるという課題があった。

【００３２】

そこで、本発明人等は日本国出願番号2002-107084(本件出願時未公開)において、ダミーデータの一部を予め試し視聴用のデータに含めながら、低品質の試し視聴ができるようにしておき、高品質化を行なう場合にダミーデータを置き換える高品質化用ファイル中の真のデータ量を減らすことによって、高品質化のためにかかる時間を短くする提案を行なった。そのための具体的な方法としては、例えば、どの帯域までの符号化を行なうのかを記録した符号化ユニット数が元の符号列に含まれる場合、この値にダミーとして小さな値を元の符号列に書き込み、符号列をそれにあわせて狭帯域再生されるように構成し、デコーダが無視する部分にダミーでない真の符号化情報の一部を記録する方法を提案した。これにより、この符号列に変更を加えて広帯域再生して高品質化する場合に必要なデータ量を減らすことができる。

【００３３】

なお、高品質化用データは暗号化することにより、高品質化のために、そのデータ販売すれば、例えば、ネットワーク上で取り引きすることが可能となる。

【００３４】

【発明が解決しようとする課題】

しかしながら、上述の方法をとると、真の帯域情報を高品質化用ファイルに記

録する必要があるが、符号化の際に帯域幅がフレーム毎に変化すると、それが雑音となって耳につきやすいため、この真の帯域情報はあまり変動させず、殆どのフレームで同一の値に設定する場合が多い。すると、高品質化用ファイルの鍵情報を総当たり法により解読しようとした場合、規則的な位置に同じ帯域情報が現われる可能性が強くなる。そのような解析はコンピュータ等を使用して、自動的に行なうことができるため、高品質化用ファイルを解読される可能性が高くなる。

【００３５】

【課題を解決するための手段】

本発明は上記課題を鑑み、暗号化されるファイルの構成要素の内、規則的に現われるデータを分離して暗号化しない、あるいは、他のデータと別途、暗号化することにより、他の重要データの暗号が解読されることを防止するようにするものである。

【００３６】

かかる本発明よれば、以下の構成を採用することが可能である。

【００３７】

例えば、信号を符号化して得られた符号列（「原符号列」という）の少なくとも一部のフレームの符号列に基づく、再生品質が低い符号列を含む第一の符号列と、第一の符号列の再生信号の高品質化に用いる第二の符号列と、の生成と、第二の符号列の暗号化と、を含む符号列生成である。この場合、暗号化では、第二の符号列において完全にまたは殆ど規則的な値をとる第一の部分は、第一の暗号化処理で暗号化され、もしくは暗号化されず、第二の符号列において第一の部分以外の少なくとも一部（「第二の部分」という）は、第一の暗号化処理とは異なる第二の暗号化処理で暗号化される。

【００３８】

ここで、第一の部分が完全にまたは殆ど規則的な値をとるというのは、そこでとる値が例えばすべて同一であったり、一定の間隔毎に1ずつ増加するなど、所定の処理で求められたり、すべてではなくとも、所定の割合、例えば、90％以上の割合で、所定の処理で求められる値をとることをいう。

【００３９】

また、第一の暗号化処理と第二の暗号化処理とは、例えば、両者で暗号化処理のアルゴリズム或いは暗号鍵を変えることにより、異ならせることができる。さらに、第一および/または第二の部分の処理単位長は、暗号化処理アルゴリズムの処理単位の整数倍とすることにより、暗号化処理の処理速度を向上させることができる。

【００４０】

なお、第二の符号列の第一の部分は、再生帯域情報または同期信号情報の少なくとも一つを含むものとすることができる。また、第一と第二の符号列は、完全に別ビットストリーム化する必要は無く、例えば、第二の符号列の第一または第二の部分を、第一の符号列の内、通常の信号再生工程が無視する部分に埋め込むことができる。この場合、当該第二の符号列の第一または第二の部分は、例えば、第一の符号列上の決められた場所に埋め込んだり、識別コードを付加したり、或いは第二の符号列に当該第一または第二の部分の場所を示す情報を第二の符号列に含めたり等、第一の符号列のデータと何かしらの形で識別できるようにすることが好適である。

【００４１】

さらに、第一および第二の符号列の生成は、ダミーデータによる原符号列の少なくとも一部の置換を含み、第一の符号列は、ダミーデータを含み、第二の符号列は、ダミーデータで置換された原符号列の真のデータの少なくとも一部を含む、ようにすることができる。この場合、ダミーデータ化は、原符号列中のスペクトル係数に相当する部分、或いは符号化パラメータ部分等、様々な部分に対して行うことができる。例えば、本発明をオーディオ信号の配信に応用する場合、中域のスペクトル係数、高域の正規化係数情報および/または量子化精度情報、或いは量子化ユニット数等、様々なオーディオ符号列中の部分をダミー化する構成が可能である。ここで、ダミー化は、例えば、一または複数のフレーム単位で行うことができ、また該フレーム内では一または複数の部分に対して行うことができる。さらに、ダミー化される真のデータの種類によって、ダミー化のやり方或いはダミーデータの構成を変えることができる。

【００４２】

さらに、ダミーデータで置換された原符号列の真のデータの少なくとも他の一部は、第一の符号列のダミーデータとは異なる部分に含まれる構成を採用することができる。すなわち、本発明では、必ずしも真のデータの全てを第二の符号列に含める必要が無く、一部を第二の符号列に含め他の一部を第一の符号列に含める構成を採用することも可能である。この場合、第一の符号列に含められる真のデータは、例えば、暗号化、スクランブルしてもよく、また、通常のデコーダでは再生されない第一の符号列内の領域等に含め、第一の符号列の単純再生では再生されないようにすることが好ましい。

【００４３】

また、本発明によれば、暗号化された符号列の暗号解除において、暗号化前の符号列において暗号化前に完全にまたは殆ど規則的な値をとっていた第一の部分に対応する第一の暗号列を、第一の解除処理で暗号解除するまたは暗号解除しない第一の暗号解除と、暗号化前の符号列において上記第一の部分以外の少なくとも一部（「第二の部分」という）に対応する第二の暗号列を、第一の解除方法とは異なる第二の暗号解除処理で暗号解除する第二の暗号解除と、を行う構成を採用することができる。ここで、第一および/または第二の部分の処理単位長は、暗号化処理アルゴリズムの処理単位の整数倍とすることにより、暗号解除処理の処理速度を向上させることができる。

【００４４】

【発明の実施の形態】

以下、図1の具体的な構成について詳細に説明する。図1に示す圧縮データ記録及び又は再生装置において、先ず記録媒体としては、スピンドルモータ５１により回転駆動される光磁気ディスク１が用いられる。光磁気ディスク１に対するデータの記録時には、例えば光学ヘッド５３によりレーザ光を照射した状態で記録データに応じた変調磁界を磁気ヘッド５４により印加することによって、いわゆる磁界変調記録を行い、光磁気ディスク１の記録トラックに沿ってデータを記録する。また再生時には、光磁気ディスク１の記録トラックを光学ヘッド５３によりレーザ光でトレースして磁気光学的に再生を行う。

【００４５】

光学ヘッド５３は、例えば、レーザダイオード等のレーザ光源、コリメータレンズ、対物レンズ、偏光ビームスプリッタ、シリンドリカルレンズ等の光学部品及び所定パターンの受光部を有するフォトディテクタ等から構成されている。この光学ヘッド５３は、光磁気ディスク１を介して上記磁気ヘッド５４と対向する位置に設けられている。光磁気ディスク１にデータを記録するときには、後述する記録系のヘッド駆動回路６６により磁気ヘッド５４を駆動して記録データに応じた変調磁界を印加すると共に、光学ヘッド５３により光磁気ディスク１の目的トラックにレーザ光を照射することによって、磁界変調方式により熱磁気記録を行う。またこの光学ヘッド５３は、目的トラックに照射したレーザ光の反射光を検出し、例えばいわゆる非点収差法によりフォーカスエラーを検出し、例えばいわゆるプッシュプル法によりトラッキングエラーを検出する。光磁気ディスク１からデータを再生するとき、光学ヘッド５３は上記フォーカスエラーやトラッキングエラーを検出すると同時に、レーザ光の目的トラックからの反射光の偏光角（カー回転角）の違いを検出して再生信号を生成する。

【００４６】

光学ヘッド５３の出力は、ＲＦ回路５５に供給される。このＲＦ回路５５は、光学ヘッド５３の出力から上記フォーカスエラー信号やトラッキングエラー信号を抽出してサーボ制御回路５６に供給するとともに、再生信号を２値化して後述する再生系のデコーダ７１に供給する。

【００４７】

サーボ制御回路５６は、例えばフォーカスサーボ制御回路やトラッキングサーボ制御回路、スピンドルモータサーボ制御回路、スレッドサーボ制御回路等から構成される。上記フォーカスサーボ制御回路は、上記フォーカスエラー信号がゼロになるように、光学ヘッド５３の光学系のフォーカス制御を行う。また上記トラッキングサーボ制御回路は、上記トラッキングエラー信号がゼロになるように光学ヘッド５３の光学系のトラッキング制御を行う。さらに上記スピンドルモータサーボ制御回路は、光磁気ディスク１を所定の回転速度（例えば一定線速度）で回転駆動するようにスピンドルモータ５１を制御する。また、上記スレッドサ

ーボ制御回路は、システムコントローラ５７により指定される光磁気ディスク１の目的トラック位置に光学ヘッド５３及び磁気ヘッド５４を移動させる。このような各種制御動作を行うサーボ制御回路５６は、該サーボ制御回路５６により制御される各部の動作状態を示す情報をシステムコントローラ５７に送る。

【００４８】

システムコントローラ５７にはキー入力操作部５８や表示部５９が接続されている。このシステムコントローラ５７は、キー入力操作部５８による操作入力情報により操作入力情報により記録系及び再生系の制御を行う。またシステムコントローラ５７は、光磁気ディスク１の記録トラックからヘッダータイムやサブコードのQデータ等により再生されるセクタ単位のアドレス情報に基づいて、光学ヘッド５３及び磁気ヘッド５４がトレースしている上記記録トラック上の記録位置や再生位置を管理する。さらにシステムコントローラ５７は、本圧縮データ記録再生装置のデータ圧縮率と上記記録トラック上の再生位置情報とに基づいて表示部５９に再生時間を表示させる制御を行う。

【００４９】

この再生時間表示は、光磁気ディスク１の記録トラックからいわゆるヘッダータイムやいわゆるサブコードQデータ等により再生されるセクタ単位のアドレス情報（絶対時間情報）に対し、データ圧縮率の逆数（例えば１／４圧縮のときには４）を乗算することにより、実際の時間情報を求め、これを表示部５９に表示させるものである。なお、記録時においても、例えば光磁気ディスク等の記録トラックに予め絶対時間情報が記録されている（プリフォーマットされている）場合に、このプリフォーマットされた絶対時間情報を読み取ってデータ圧縮率の逆数を乗算することにより、現在位置を実際の記録時間で表示させることも可能である。

【００５０】

次にこのディスク記録再生装置の記録系において、入力端子６０からのアナログオーディオ入力信号ＡINがローパスフイルタ６１を介してＡ／Ｄ変換器６２に供給され、このＡ／Ｄ変換器６２は上記アナログオーディオ入力信号ＡINを量子化する。Ａ／Ｄ変換器６２から得られたデジタルオーディオ信号は、ＡＴＣ（Ad

aptive Transform Coding）エンコーダ６３に供給される。また、入力端子６７からのデジタルオーディオ入力信号ＤＩＮがデジタル入力インターフェース回路６８を介してＡＴＣエンコーダ６３に供給される。ＡＴＣエンコーダ６３は、上記入力信号ＡＩＮを上記Ａ／Ｄ変換器６２により量子化した所定転送速度のデジタルオーディオＰＣＭデータについて、所定のデータ圧縮率に応じたビット圧縮（データ圧縮）処理を行うものであり、ＡＴＣエンコーダ６３から出力される圧縮データ（ＡＴＣデータ）は、メモリ６４に供給される。例えばデータ圧縮率が１／８の場合について説明すると、ここでのデータ転送速度は、上記標準のＣＤ－ＤＡのフオーマットのデータ転送速度（７５セクタ／秒）の１／８（9.375セクタ／秒）に低減されている。

【００５１】

次にメモリ６４は、データの書き込み及び読み出しがシステムコントローラ５７により制御され、ＡＴＣエンコーダ６３から供給されるＡＴＣデータを一時的に記憶しておき、必要に応じてディスク上に記録するためのバッファメモリとして用いられている。すなわち、例えばデータ圧縮率が１／８の場合において、ＡＴＣエンコーダ６３から供給される圧縮オーディオデータは、そのデータ転送速度が、標準的なＣＤ－ＤＡフォーマットのデータ転送速度（７５セクタ／秒）の１／８、すなわち９．３７５セクタ／秒に低減されており、この圧縮データがメモリ６４に連続的に書き込まれる。この圧縮データ（ＡＴＣデータ）は、前述したように８セクタにつき１セクタの記録を行えば足りるが、このような８セクタおきの記録は事実上不可能に近いため、後述するようなセクタ連続の記録を行うようにしている。

【００５２】

この記録は、休止期間を介して、所定の複数セクタ（例えば３２セクタ＋数セクタ）から成るクラスタを記録単位として、標準的なＣＤ－ＤＡフォーマットと同じデータ転送速度（７５セクタ／秒）でバースト的に行われる。すなわちメモリ６４においては、上記ビット圧縮レートに応じた９．３７５（＝７５／８）セクタ／秒の低い転送速度で連続的に書き込まれたデータ圧縮率１／８のＡＴＣオーディオデータが、記録データとして上記７５セクタ／秒の転送速度でバースト

的に読み出される。この読み出されて記録されるデータについて、記録休止期間を含む全体的なデータ転送速度は、上記９．３７５セクタ／秒の低い速度となっているが、バースト的に行われる記録動作の時間内での瞬時的なデータ転送速度は上記標準的な７５セクタ／秒となっている。従って、ディスク回転速度が標準的なＣＤ－ＤＡフォーマットと同じ速度（一定線速度）のとき、該ＣＤ－ＤＡフォーマットと同じ記録密度、記憶パターンの記録が行われることになる。

【００５３】

メモリ６４から上記７５セクタ／秒の（瞬時的な）転送速度でバースト的に読み出されたＡＴＣオーディオデータすなわち記録データは、エンコーダ６５に供給される。ここで、メモリ６４からエンコーダ６５に供給されるデータ列において、１回の記録で連続記録される単位は、複数セクタ（例えば３２セクタ）から成るクラスタ及び該クラスタの前後位置に配されたクラスタ接続用の数セクタとしている。このクラスタ接続用セクタは、エンコーダ６５でのインターリーブ長より長く設定しており、インターリーブされても他のクラスタのデータに影響を与えないようにしている。

【００５４】

エンコーダ６５は、メモリ６４から上述したようにバースト的に供給される記録データについて、エラー訂正のための符号化処理（パリティ付加及びインターリーブ処理）やＥＦＭ符号化処理などを施す。このエンコーダ６５による符号化処理の施された記録データが磁気ヘッド駆動回路６６に供給される。この磁気ヘッド駆動回路６６は、磁気ヘッド５４が接続されており、上記記録データに応じた変調磁界を光磁気ディスク１に印加するように磁気ヘッド５４を駆動する。

【００５５】

また、システムコントローラ５７は、メモリ６４に対する上述の如きメモリ制御を行うとともに、このメモリ制御によりメモリ６４からバースト的に読み出される上記記録データを光磁気ディスク１の記録トラックに連続的に記録するように記録位置の制御を行う。この記録位置の制御は、システムコントローラ５７によりメモリ６４からバースト的に読み出される上記記録データの記録位置を管理して、光磁気ディスク１の記録トラック上の記録位置を指定する制御信号をサー

ボ制御回路５６に供給することによって行われる。

【００５６】

次に再生系について説明する。この再生系は、上述の記録系により光磁気ディスク１の記録トラック上に連続的に記録された記録データを再生するためのものであり、光学ヘッド５３によって光磁気ディスク１の記録トラックをレーザ光でトレースすることにより得られる再生出力がＲＦ回路５５により２値化されて供給されるデコーダ７１を備えている。この時光磁気ディスクのみではなく、Compact Discと同じ再生専用光ディスクの読み出しも行なうことができる。

【００５７】

デコーダ７１は、上述の記録系におけるエンコーダ６５に対応するものであって、ＲＦ回路５５により２値化された再生出力について、エラー訂正のための上述の如き復号処理やＥＦＭ復号処理などの処理を行い、上述のデータ圧縮率１／８のＡＴＣオーディオデータを、正規の転送速度よりも早い７５セクタ／秒の転送速度で再生する。このデコーダ７１により得られる再生データは、メモリ７２に供給される。

【００５８】

メモリ７２は、データの書き込み及び読み出しがシステムコントローラ５７により制御され、デコーダ７１から７５セクタ／秒の転送速度で供給される再生データがその７５セクタ／秒の転送速度でバースト的に書き込まれる。また、このメモリ７２は、上記７５セクタ／秒の転送速度でバースト的に書き込まれた上記再生データがデータ圧縮率１／８に対応する９．３７５セクタ／秒の転送速度で連続的に読み出される。

【００５９】

システムコントローラ５７は、再生データをメモリ７２に７５セクタ／秒の転送速度で書き込むとともに、メモリ７２から上記再生データを上記９．３７５セクタ／秒の転送速度で連続的に読み出すようなメモリ制御を行う。また、システムコントローラ５７は、メモリ７２に対する上述の如きメモリ制御を行うとともに、このメモリ制御によりメモリ７２にバースト的に書き込まれる上記再生データを光磁気ディスク１の記録トラックから連続的に再生するように再生位置の制

御を行う。この再生位置の制御は、システムコントローラ５７によりメモリ７２から連続的に読み出される上記再生データの再生位置を管理して、光磁気ディスク１もしくは光ディスク１の記録トラック上の再生位置を指定する制御信号をサーボ制御回路５６に供給することによって行われる。

【００６０】

メモリ７２から９．３７５セクタ／秒の転送速度で連続的に読み出された再生データとして得られるＡＴＣオーディオデータは、ＡＴＣデコーダ７３に供給される。このＡＴＣデコーダ７３は、上記記録系のＡＴＣエンコーダ６３に対応するもので、例えばＡＴＣデータを８倍にデータ伸張（ビット伸張）することで１６ビットのデジタルオーディオデータを再生する。このＡＴＣデコーダ７３からのデジタルオーディオデータは、Ｄ／Ａ変換器７４に供給される。

【００６１】

Ｄ／Ａ変換器７４は、ＡＴＣデコーダ７３から供給されるデジタルオーディオデータをアナログ信号に変換して、アナログオーディオ出力信号ＡOUTを形成する。このＤ／Ａ変換器７４により得られるアナログオーディオ信号ＡOUTは、ローパスフイルタ７５を介して出力端子７６から出力される。

【００６２】

（符号化および復号化）

次に高能率圧縮符号化について詳述する。すなわち、オーディオＰＣＭ信号等の入力デジタル信号を、帯域分割符号化（ＳＢＣ）、適応変換符号化（ＡＴＣ）及び適応ビット割当ての各技術を用いて高能率符号化する技術について、図2以降を参照しながら説明する。

【００６３】

図2は本発明にかかわる音響波形信号の符号化装置の具体例を示すブロック図である。この具体例において、入力された信号波形 101 は変換手段 1101 によって信号周波数成分に 102 に変換された後、信号成分符号化手段 1102 によって各成分が符号化され、符号列生成手段 1103 によって符号列 104 が生成される。

【００６４】

図3は図2の変換手段 1101 の具体例である。図3において、信号201は、帯域分割フィルター1201によって二つの帯域に分割され、信号211、212が生成される。信号211、212は、それぞれの帯域においてMDCT等の順スペクトル変換手段1211、1212によりスペクトル信号成分 221、222に変換される。図3の 201 は図2の 101 に、図3の 221、222 は図2の 102 に対応している。図３の変換手段で、211、212 の信号の帯域幅は 201 の信号の帯域幅の1/2となっており、201 の信号の1/2に間引かれている。もちろん変換手段としてはこの具体例以外にも多数考えられ、例えば、入力信号を直接、MDCT によってスペクトル信号に変換しても良いし、MDCT ではなく、DFTやDCT によって変換しても良い。いわゆる帯域分割フィルターによって信号を帯域成分に分割することも可能であるが、本発明の方法は、多数の周波数成分が比較的少ない演算量で得られる上記のスペクトル変換によって周波数成分に変換する方法をとると都合が良い。

【００６５】

図4は図2の信号成分符号化手段 1102 の具体例で、各信号成分は、正規化手段 1301 によって所定の帯域毎に正規化が施された後、量子化精度決定手段 1302 によって計算された量子化精度に基づいて量子化手段 1303 によって量子化される。図4の 301 は図2の 102 に、図4の 304 は図2の 103 に対応しているが、ここで、304 には量子化された信号成分に加え、正規化係数情報や量子化精度情報も含まれている。

【００６６】

図5は図2の具体例の符号化装置によって生成された符号列から音響信号を出力する復号装置の具体例を示すブロック図である。この具体例において、符号列 401 から符号列分解手段 1401 によって各信号成分の符号が抽出され、それらの符号から信号成分復号手段 1402 によって各信号成分が復元された後、逆変換手段 1403 によって音響波形信号 404 が出力される。

【００６７】

図6は図5の逆変換手段 1403 の具体例であるが、これは図3の変換手段の具体例に対応したもので、信号501、502から逆スペクトル変換手段1501、1502によって得られた各帯域の信号511、512が帯域合成フィルター1511によって合成されて

いる。図6の 501、502は図5の 403 に図6の 521 は図5の 404 に対応している。

【００６８】

図7は図5の信号成分復号手段 1402 の具体例で、図7の 551 は図5の 402 に、図7の553は図5の 403 に対応する。551の各スペクトル信号は逆量子化手段 1551 によって逆量子化された後、逆正規化手段 1552 によって逆正規化される。

【００６９】

図8は図2に示される符号化装置において行うことができる符号化方法例について説明を行なうための図である。この図の例において、スペクトル信号は図3の変換手段によって得られたものであり、図8は MDCT のスペクトルの絶対値をレベルをdBに変換して示したものである。入力信号は所定の時間ブロック毎に64個のスペクトル信号に変換されており、それが[b1]から[b8]の8つの帯域(以下、これを符号化ユニットと呼ぶ)にまとめて正規化および量子化が行なわれる。量子化精度は周波数成分の分布の仕方によって符号化ユニット毎に変化させることにより、音質の劣化を最小限に押さえる聴覚的に効率の良い符号化が可能である。

【００７０】

図9は上述のように符号化された信号を記録媒体に記録する場合の具体例を示したものである。この具体例では、各フレームの先頭に同期信号を含む固定長のヘッダがついており、ここに符号化ユニット数も記録されている。ヘッダの次には量子化精度情報が上記符号化ユニット数だけ記録され、その後に正規化精度データが上記符号化ユニット数だけ記録されている。正規化および量子化されたスペクトル係数情報はその後に記録されるが、フレームの長さが固定の場合、スペクトル係数情報の後に、空き領域ができても良い。この図の例は、図8のスペクトル信号を符号化したもので、量子化精度情報としては最低域の符号化ユニットの6ビットから最高域の符号化ユニットの2ビットまで図示されたように割り当てられ、正規化係数情報としては、最低域の符号化ユニットの46という値から最高域の符号化ユニットの22までの値まで図示されたように割り当てられている。なお、この正規化係数情報としては、ここではdB値に比例した値が用いられている。

【００７１】

以上述べた方法に対して、さらに符号化効率を高めることが可能である。例えば、量子化されたスペクトル信号のうち、頻度の高いものに対しては比較的短い符号長を割り当て、頻度の低いものに対しては比較的長い符号長を割り当てることによって、符号化効率を高めることができる。また例えば、変換ブロック長を長くとることによって、量子化精度情報や正規化係数情報といったサブ情報の量を相対的に削減でき、また周波数分解能を上がるので、周波数軸上で量子化精度をよりこまやかに制御できるため、符号化効率を高めることができる。

【００７２】

さらにまた、本発明人らによる発明、国際公開番号WO94/28633(対応米国特許番号US5717821）では、スペクトル信号から聴感上特に重要なトーン性の成分、すなわち特定の周波数周辺にエネルギーが集中している信号成分、を分離して、他のスペクトル成分とは別に符号化する方法が提案されており、これにより、オーディオ信号等を聴感上の劣化を殆ど生じさせずに高い圧縮率で効率的に符号化することが可能になっている。

【００７３】

図１０は、このような方法を用いて符号化を行なう場合の方法を説明するための図で、スペクトル信号から、特にレベルが高いものをトーン成分、例えばトーン成分Ｔｎ１～Ｔｎ３として分離して符号化する様子を示している。各トーン成分Ｔｎ１～Ｔｎ３に対しては、その位置情報、例えば位置データPos１～Pos３も必要となるが、トーン成分Ｔｎ１～Ｔｎ３を抜き出した後のスペクトル信号は少ないビット数で量子化することが可能となるので、特定のスペクトル信号にエネルギが集中する信号に対して、このような方法をとると、特に効率の良い符号化が可能となる。

【００７４】

図11はそのようにトーン性成分を分離して符号化する場合の、図2の信号成分符号化手段1102 の構成を示したものである。図2の変換手段 1101 の出力102 に相当する信号601 はトーン成分分離手段 1601 によって、トーン成分602と非トーン成分603に分離され、それぞれ、トーン成分符号化手段 1602 および非トーン成分符号化手段 1603 によって符号化される。この結果、トーン成分／非トー

ン成分の符号列604、605が生成される。トーン成分符号化手段 1602 および非トーン成分符号化手段 1603 は、図4と同様の構成をとるが、トーン成分符号化手段 1602はトーン成分の位置情報の符号化も行なう。

【００７５】

同様に図12はそのようにトーン性成分を分離して符号化されたものを復号する場合の、図5の信号成分復号手段 1402 の構成をしめしたものである。信号701、702は、それぞれ、トーン成分復号化手段1701、非トーン成分復号化手段1502により、スペクトル信号703、704に復号化される。スペクトル信号703、704は、スペクトル信号合成手段1703によって合成され、復号後の信号705が生成される。

【００７６】

図１３は、上述のように符号化された信号を記録媒体に記録する場合の具体例を示したものである。この具体例では、トーン成分を分離して符号化しており、その符号列がヘッダ部と量子化精度情報ＱＮの間の部分に記録されている。トーン成分列に対しては、先ず、トーン成分数情報ＴＮが記録され、次に各トーン成分のデータが記録されている。トーン成分のデータとしては、位置情報Ｐ、量子化精度情報ＱＮ、正規化係数情報ＮＰ、スペクトル係数情報ＳＰが挙げられる。この具体例ではさらに、スペクトル信号に変換する変換ブロック長を、図９の具体例の場合の２倍にとって周波数分解能も高めてあり、さらに可変長符号も導入することによって、図９の具体例に比較して、同じバイト数のフレームに２倍の長さに相当する音響信号の符号列を記録している。

【００７７】

（試聴用ファイルと高品質化用ファイルの生成・再生等）

国際出願番号PCT/JP02/01106の符号化方法では、例えば、図9のように符号化されるべきところに、図14に示すように、量子化精度情報ＱＮの内のダミーの量子化精度データとして、高域側の４つの符号化ユニットに対して０ビット割り当てを示すデータを符号化し、また、正規化係数情報ＮＰの内のダミーの正規化係数データとして高域側の４つの符号化ユニットには最小の値の正規化係数情報０を符号化する（この具体例では正規化係数はｄＢ値に比例した値をとるものとする）。このように、高域側の量子化精度情報を０にすることによって、試聴時に無

視されるデータ係数情報の領域Ｎeg、実際には図１４の領域Ｎegの部分のスペクトル係数情報は無視され、これを通常の再生装置で再生すると図15に示したようなスペクトルを持つ狭帯域のデータが再生される。また、正規化係数情報もダミーのデータを符号化することによって、量子化精度情報を推測して不正に高品質再生をすることが一層、困難になる。

【００７８】

さらに、図14の例においては斜線で示された中域のスペクトル・データの一部はダミーデータ（ダミースペクトル係数情報ＤＳＰ）に置き換えられており、不正にこの試聴用ファイルを広帯域化することはさらに困難になっている。特にここでは、可変長符号を用いてスペクトル係数情報を符号化し、低域側からスペクトル係数情報を符号化することにしているため、中域のスペクトルをダミーデータにすることにより、それより高いスペクトル係数情報はすべて正しく読めなくなっている。ただし、試聴時には、これらの帯域の音はダミーの正規化係数情報のためにミューティングされているため、不快な雑音が聞こえることはない。

【００７９】

なお、上記の例では、量子化精度情報と正規化係数情報の両者をダミーデータで置き換えているが、どちらか一方のみをダミーデータで置き換えるようにしても良い。量子化精度情報のみを0ビットデータのダミーデータとした場合には、やはり図15に示したようなスペクトルを持つ狭帯域のデータが再生される。一方、正規化係数情報のみを0の値を持つダミーデータとした場合には、図16に示したようなスペクトルを持つことになり、高域側のスペクトルは厳密には0にはならないが、可聴性という観点からは実質的には0と同じであり、本出願においては、この場合も含めて狭帯域信号と呼ぶことにする。

【００８０】

量子化精度情報および正規化係数情報のうち、どのデータをダミーデータにするかという点に関しては、これらの真の値を推測されて高品質再生されてしまうというリスクに関して差異がある。量子化精度情報と正規化係数情報の両者がダミーデータとなっている場合、これらの真の値を推測するためのデータが全く無いため、一番、安全である。量子化精度情報のみダミーデータにした場合には、

例えば、元のビット割り当てアルゴリズムが正規化係数を元に量子化精度情報を求めるものである場合、正規化係数情報を手掛かりにして量子化精度情報を推測される可能性があるため、リスクは比較的高くなる。これに対して、量子化精度情報から正規化係数情報を求めることは比較的困難であるから、正規化係数情報のみをダミーデータとする方法は量子化精度情報のみをダミーデータとする方法と比較してリスクは低くなる。なお、帯域によって、量子化精度情報または正規化係数情報を選択的にダミーデータとするようにしても良い。

【００８１】

何れにしても、信号の内容に立ち入った比較的大きなデータを推測することは、通常の暗号化で用いる比較的短い鍵長を解読することに比べて困難であり、例えば、その曲の著作権者の権利が不正に侵されるリスクは低くなると言える。また、仮にある曲に対して、ダミーデータを推測されても、暗号アルゴリズムの解読方法が知られる場合と異なり、他の曲に対して被害が拡大する恐れはないので、その点からも特定の暗号化を施した場合よりも安全性が高いと言うことができる。

【００８２】

図17は国際出願番号PCT/JP02/01106の方法による再生手段の例を示すブロック図で、図5の復号手段を改良したものである。図17において、801は一部をダミーデータで置き換えられた符号列であり、ここでは、高域側の量子化精度情報および正規化係数情報がダミーデータになっているものとする。これが先ず符号列分解手段 1801 によって符号列の内容が分解され、802として符号列書き換え手段 1802 に送られる。符号列書き換え手段 1802 は制御手段 1805 を通じて真の量子化精度情報および正規化係数情報806を807として受け取り、これにより、802のうちのダミーの量子化精度情報および正規化係数情報の部分を書き換え、その結果を信号成分復号手段 1803 に送る。信号成分復号手段 1803 は、このデータをスペクトル・データ804に復号し、逆変換手段 1804 はこれを時系列データ 805 に変換して、広い帯域の高音質のオーディオ信号を再生する。ここで、真の量子化精度情報および正規化係数情報806は暗号化することによって、安全性を高めるようにしておくことが望ましいことは言うまでもない。

【００８３】

図18は、図17の807の真の情報のフォーマットの具体例を示したもので、図14に示されるN番フレームの情報を図9に示す情報に変更するためのものである。これにより、ダミーデータの入ったままの符号列では、図15に示されるスペクトルを持つ再生音が図8に示すスペクトルを持つ再生音に変化することになる。ここで、これらの情報は暗号化することによって安全性を高めることが望ましいのは既に述べたとおりであり、以下、これらの高品質化のためのデータ列は特に述べない限り暗号化されているものとする。

【００８４】

図19は国際出願番号PCT/JP02/01106の方法による記録手段の例を示すブロック図である。図19において、821は一部をダミーデータで置き換えられた符号列であり、ここでは、高域側の量子化精度情報および正規化係数情報がダミーデータになっているものとする。これが先ず符号列分解手段 1821 によって符号列の内容が分解され、822として符号列書き換え手段 1822 に送られる。符号列書き換え手段 1822 は制御手段 1824 を通じて真の量子化精度情報および正規化係数情報825を826として受け取り、これにより、822のうちのダミーの量子化精度情報および正規化係数情報の部分を書き換え、その結果を記録手段 1823 に送り、これを記録メディアに記録する。なお、ここで 824 の符号列を記録する記録メディアは、元々821の符号列を記録していた記録メディアであるとしても良い。

【００８５】

図20は、図10に示すようにトーン成分を分離し、図13に示すように符号化した場合に、ダミーデータを置き換える情報のフォーマットの具体例を示したものである。これにより、図15に示されるスペクトルを持つ再生音が図10に示すスペクトルを持つ再生音に変化することになる。なお、図20の例はトーン性の成分を分離して符号化した場合の高品質化のための追加ファイルであり、元の試聴用ファイルでは、所定の帯域以上にあるトーン性の成分の正規化係数情報には実質的に大きさが0であるダミーデータが符号化されている。

【００８６】

さて、以上、本発明に適用可能な符号化方法の説明をおこなったが、以上説明

した方法をオーディオに適用したものは、比較的低品質のオーディオ信号は内容の試聴用として自由に聞くことができるようにし、高品質のオーディオ信号は、試聴用ファイルに比較してデータ量の小さいの追加ファイルを購入などして入手することで聞けるようにするものである。

【００８７】

しかしながら、高品質化のための追加ファイルのデータ量は、日本国出願番号2002-107084(本件出願時未公開)の方法により、さらに小さくすることが可能である。高品質化のための追加データの量を減らすことは、追加データを通信手段などで入手する時間、ひいては、ユーザが高品質オーディオの購入を決めてから実際にそれを得るまでの時間を短縮する上で有効である。

以下、これをトーン性の成分を分離しない場合について説明を行なうが、もちろん、トーン性の成分を分離した場合についても、容易に同様の方法を拡張することが可能である。

【００８８】

図21は日本国出願番号2002-107084(本件出願時未公開)による試聴用ファイルの符号列のフォーマットの具体例を示したものである。この具体例においては、符号化ユニット数ＵＮが、試聴用として狭帯域再生されるように、予め４に指定（ＵＮ＝４）されており、実際に、本来のフォーマットで量子化精度情報ＱＮ、正規化係数情報ＮＰが符号化される部分には、４つ分のデータしか符号化されていない。このため、その次に、広帯域の再生に必要なスペクトル係数情報ＳＰが、例えば全て符号化されているとしても、試聴時には、上記符号化ユニットの４つ分に相当するスペクトル係数情報よりも後方に符号化されたデータ（領域Ｎegのデータ）は、全て無視される。また、フレームの最後の部分からは、正規の位置には符号化されていなかった高域側の量子化精度情報ＱＮ’、正規化係数情報ＮＰ’が符号化されている。ここでは正規の位置に符号化されている量子化精度情報ＱＮ、正規化係数情報ＮＰは低域側の分しか符号化されていないので、これらの高域側の情報を符号化する領域を確保することが可能である。また、スペクトル係数情報の符号化に可変長符号が使用されており、試聴時に無視される中域のスペクトル係数情報の一部がダミーデータ（ダミースペクトル係数情報ＤＳＰ

）に置き換えられている。

【００８９】

なお、この具体例では、量子化精度情報、正規化係数情報は、符号列の開始位置が簡単にわかるよう、フレームの後端から前方に向かって低域側から順番に符号化されているが、もちろん、他の順番であっても良い。ただし、特にフレーム長が固定的である場合には、このようにフレームの後ろ側から真のデータを符号化することは、その場所を特定する上で極めて都合が良い。また、この具体例では、試聴時に無視される中域のスペクトル係数情報の一部がダミーデータに置き換えられている。このデータは試聴時には無視されるので耳障りな雑音が発生することはない。なお、この具体例では、スペクトル係数情報の符号化に可変長符号が使用されているものとしているので、中域のデータがわからないとそれ以上の帯域のスペクトル係数情報はすべて読めなくなり、安全性が高くなっている。

【００９０】

図22は図21の試聴用ファイルの符号列を高品質化するための追加ファイルのデータの1フレーム分のフォーマットの具体例を示したものである。この具体例では、各フレーム毎に先ず、真の符号化ユニット数が記録してあり、次に中域のダミーのスペクトル係数情報を置き換える真のスペクトル係数情報が符号化されている。

【００９１】

図23は日本国出願番号2002-107084(本件出願時未公開)の方法による再生手段の例を示すブロック図である。図23において、841は一部をダミーデータで置き換えられた符号列であり、ここでは、符号化ユニット数および中域のスペクトル係数情報がダミーデータになっているものとする。これが先ず符号列分解手段 1841 によって符号列の内容が分解され、842として制御手段1845に送られる。一方、制御手段1845には、図22に示されるフォーマットの符号列846も送られ、842のデータと合わせて、広帯域化した符号列を作成し、信号成分復号手段1842に843として送る。信号成分復号手段 1842 は、このデータをスペクトル・データ844に復号し、逆変換手段 1843 はこれを時系列データ 845 に変換して、広い帯域の高音質のオーディオ信号を再生する。

【００９２】

図24は日本国出願番号2002-107084(本件出願時未公開)の方法による記録手段の例を示すブロック図である。図24において、861は一部をダミーデータで置き換えられた符号列であり、ここでは、符号化ユニット数および中域のスペクトル係数情報がダミーデータになっているものとする。これが先ず符号列分解手段 1861 によって符号列の内容が分解され、862として制御手段 1863 に送られる。一方、制御手段1863には、図22に示されるフォーマットの符号列865も送られ、862のデータと合わせて、広帯域化した符号列を作成し、記録手段1862に863として送る。記録手段1862は、これを記録メディアに記録する。なお、ここで864の符号列を記録する記録メディアは、元々861の符号列を記録していた記録メディアであるとしても良い。

【００９３】

図25は日本国出願番号2002-107084(本件出願時未公開)の方法で、ソフトウェアを用いて再生を行なう方法の流れを示したフローチャートの例である。先ず、S11においてダミーデータを含んだ符号列の分解を行ない、次にS12において、高音質再生を行なうかどうかを判断する。高音質再生を行なう場合には、S13において、真の符号化ユニット数の符号列への埋め込みを行ない、高音質再生を行なわない場合には、S19に進む。S14においては、真の量子化精度情報、正規化係数情報の読み出しを行ない、S15においては、真のスペクトル係数情報の読み出しを行なう。次にS16においてダミーデータを含むスペクトル係数情報の読み出しを行なった後、S17において、真の量子化精度情報、正規化係数情報の符号列への埋め込みを行なう。その後、S18において、真の量子化精度情報、正規化係数情報の符号列への埋め込みが終わった次の位置から、真のスペクトル情報を、予め、S15、S16で読み出してあった情報から作成し、それを符号列に埋め込む。こうしてできた符号列に対して、S19において信号成分の復号を行ない、S20において、その信号成分を時系列信号に変換し、処理を終了する。

【００９４】

図26は日本国出願番号2002-107084(本件出願時未公開)の方法で、ソフトウェアを用いて記録を行なう方法の流れを示したフローチャートの例である。先ず、

S21において高音質記録を行なうかどうかを判断する。高音質記録を行なう場合には、次にS22において、ダミーデータを含んだ符号列の分解を行ない、高音質再生を行なわない場合には、S29に進む。S23においては、真の符号化ユニット数の符号列への埋め込みを行ない、次にS24において、真の量子化精度情報、正規化係数情報の読み出しを行ない、S25においては、真のスペクトル係数情報の読み出しを行なう。次にS26においてダミーデータを含むスペクトル係数情報の読み出しを行なった後、S27において、真の量子化精度情報、正規化係数情報の符号列への埋め込みを行なう。その後、S28において、真の量子化精度情報、正規化係数情報の符号列への埋め込みが終わった次の位置から、真のスペクトル情報を、予め、S25、S26で読み出してあった情報から作成し、それを符号列に埋め込む。こうしてできた符号列に対して、S29において符号列の記録を行ない、処理を終了する。

【００９５】

図27は、日本国出願番号2002-107084(本件出願時未公開)の方法で、例えば、64フレーム毎に一つの鍵で高品質化用ファイルを暗号化する場合のデータの内容の例を図示したものである。既に述べたように、フレームによって頻繁に帯域が変化すると、非常に聞きづらい音になってしまうため、多くのフレームにおいて、符号化ユニット数は同一であることが多く、通常は一定の符号化ユニット数で、例外的に変化が生じる場合が極めて多くなるが、例外的にでも、符号化ユニット数は変化することもありうるので、そのデータを省略することはできない。図27の例では、(M+62)番フレームでの真の符号化ユニット数は7で、他のフレームでは符号化ユニット数が8となっている。すると、例えば、鍵の総当たり法で解読を試みた場合、殆どの符号化ユニット数が同一になる場合は、非常に限られてくるため、自動的に、鍵の候補を非常に少ないものに絞ることができるようになってしまい、それらの少ない候補の中から真の高品質化用ファイルを選択することが比較的容易になってしまう。

【００９６】

図28はこれを解決するための本発明による高品質化用ファイルの暗号化の方法の具体例を示したものである。図28の例では、各フレームの真のデータの内、殆

どのものが同一の値をとる真の符号化ユニット数の情報をまとめてA領域に並べ、それ以外のランダムな値をとる真の中域スペクトル・データ符号列の情報をまとめてB領域に並べ、このうち、B領域のデータについては暗号化を施し、A領域のデータについては別の暗号化を施すか、あるいは、全く暗号化を施さない。このようにすると、A領域に記録されたデータは、解読者に知られてしまう可能性が高いが、B領域のデータに関しては、例えば、鍵の総当たり法による解読を行なおうとしても、真のデータはランダムな値をとるため、解読者はどれが正解であるかを知ることができず、膨大な数のすべての候補に対して実際に音を聞いてみるなど、非現実的な方法でしか正解を確かめることができなくなってしまい、高い安全性を保つことができる。なお、もちろん、A領域のデータ・フォーマットとしては、例えば、例外的な符号化ユニット数をとるフレーム番号とその符号化ユニット数のデータとその他のフレームの符号化ユニット数のデータを符号化するなど、より短い符号で表すことも可能である。

【００９７】

またここでは、真の符号化ユニット数情報を高品質化用ファイルの一部として符号化しているようにしているが、符号化ユニット数情報を元の試聴用ファイルの各フレームの符号列のうちの、実際にはデコーダが無視する領域に符号化しておくようにすることも可能である。この場合、この真の符号化ユニット数情報を符号列に含める領域を確保するためには、例えば、予め、そのフレームを高品質符号化するのに用いるビット数を、符号化ユニット数情報分少ないものとして符号化しておくようにすれば良い。このような方法も本発明の方法に含まれるものである。

【００９８】

なお、本発明人等は日本国出願番号2002-146731(本件出願時未公開)において、ダミーデータを含む第一の符号列の一部を、第二の符号列(高品質化用ファイル)に基づいて変更を加えて再生や記録を行なう方法において、上記第一の符号列中の一部のフレームのみ、上記第一の符号列のダミーデータの一部を置き換える真のデータを上記第一の符号列中に埋め込んでいることを特徴とする情報再生・記録方法を提案し、これにより、安全性を高いレベルに維持したまま、第二の

符号列(高品質化用ファイル)のデータ量を減らすことを提案しているが、本発明の方法は、もちろん、このような場合にも、適用することが可能である。

【００９９】

図29は、本発明の方法により、高品質な再生が可能な符号列を、試聴用ファイルと高品質化ファイルに分解する信号処理手段の具体例を示した図である。この具体例においては、先ず、高品質な再生が可能な符号列 881 を符号列分解手段 1881 に入力し、試聴用ファイル 888 とその高品質化を行なうデータ 882 に分解する。次に高品質化を行なうデータ 882 は、高品質化データ分離手段 1882 に送られ、高品質データの符号列のうち、殆ど規則的な値をとる符号列部分 883 とそれ以外の部分 884 に分離する。この符号列部分 884 は暗号化手段B 1884 に送られ、制御手段 1886 によって発生された一連のフレームを暗号化する鍵 890 を使用して暗号化され、暗号化された符号列部分 886 は高品質化符号列統合手段 1885 に送られる。

【０１００】

一方、殆ど規則的な値をとる符号列部分 883 は暗号化手段A 1883 に送られ、暗号化手段B 1884 で上記一連のフレームを暗号化した鍵とは別の、制御手段 1886 によって発生された鍵 889 を使用して暗号化が行なわれ、暗号化された符号列部分 885 は高品質化符号列統合手段 1885 に送られる。ただし、既に説明したように、暗号化手段A 1883 は省略して、殆ど規則的な値をとる符号列部分 883 は平文のまま、符号列部分 885 として高品質化符号列統合手段 1885 に送るようにしても良い。高品質化符号列統合手段 1885 は、符号列 885 と符号列 886 を合成して、例えば、図28に示すような暗号化された高品質化ファイル 887 を作成する。なお、鍵 889、890 は高品質化ファイルのサーバにも送られる。

【０１０１】

図30は、図29に示した信号処理手段の具体例の出力である試聴用ファイルとその暗号化された高品質化ファイルとその鍵から高品質なオーディオ・データを出力する信号処理手段の具体例を示したものである。先ず、図29の高品質化ファイル 887 に対応する 901 が高品質化符号列分離手段 1901 に入力されると、高品質化符号列分離手段 1901 は、それを暗号化された元々殆ど規則的な値をとる符

号列部分 902 と暗号化されたその他の符号列部分 903 に分離する。暗号化されたその他の符号列部分 903 は暗号復号手段B 1903 で図29の暗号化手段B 1884 で使用された鍵 890 に対応する鍵 911 で暗号を復号された後、符号列部分 905 として高品質化手段 1904 に送られ、暗号化された元々殆ど規則的な値をとる符号列部分 902 は暗号復号手段A 1902 に送られて、図29の暗号化手段A 1883 で使用された鍵 889 に対応する鍵 910 で暗号を復号された後、符号列部分 904 として高品質化手段 1904 に送られる。

【０１０２】

ただし、図29の暗号化手段A が省略されている場合には、符号列部分 902 は暗号化されておらず、暗号復号手段A 1902 は省略されて、符号列部分 902 は 904 として、直接、高品質化手段 1904 に入力される。高品質化手段 1904 には、図29の 888 に対応する試聴用ファイル 906 も入力され、符号列部分 904、905を使用して、符号列 906 が高品質化処理され、高品質な信号に逆変換される符号列 907 が出力される。

【０１０３】

なお、高品質化ファイルのサーバと、図30の高品質化手段の間での暗号の復号鍵 910、911 の受け渡しに関しては、よく知られているように、例えば、両者が共有する秘密鍵と乱数発生器を備えているものとして次のように行なうことができる。先ず、高品質化ファイルのサーバが乱数を発生し、これを図30の高品質化手段と共有している秘密鍵を用いて例えばDESで暗号化して図30の高品質化手段に送信する。次に、図30の高品質化手段は、上記の秘密鍵を用いてこれを復号し、複合された値に1を加えた値を上記の秘密鍵を用いて、例えばDESで暗号化して高品質化ファイルのサーバに送信する。高品質化ファイルのサーバはこれを復号し、自身が発生させた乱数より1だけ大きい値が得られるかどうかをチェックする。もし、チェックの結果が正しければ、高品質化ファイルのサーバは図30の高品質化手段が正しい秘密鍵の値を保持している正当なものであると判断する。次に高品質化ファイルのサーバと図30の高品質化手段は、上記の役割を交代して行ない、図30の高品質化手段は高品質化ファイルのサーバが正当なものであることをチェックする。

【０１０４】

ここでその正当性がチェックできたら、図30の高品質化手段は乱数 R を発生し、Rを例えば、先に図30の高品質化手段が高品質化ファイルサーバに送った乱数を鍵としてDESで暗号化して送る。高品質化サーバはこの R を復号し、このRを鍵として、高品質化ファイルを暗号化する鍵を図30の高品質化手段に送る。もちろん、高品質化ファイルの鍵がファイルの部分によって複数存在する場合には、例えば、上記の送信方法を乱数 R の値を変えて繰り返すようにして、それぞれ別の鍵で高品質化ファイルのそれぞれの部分の鍵を送信するようにしても良い。なお、上記の例においては、図30の高品質化手段において、秘密鍵は制御手段 1905 内の十分に保護されたROMに格納されており、また制御手段 1905 は乱数発生手段を内蔵しているものとする。またもちろん、高品質化ファイルサーバにおいても秘密鍵は十分に保護されており、高品質化ファイルサーバも乱数発生手段を装備しているものとする。

【０１０５】

図31は、本発明の方法により、ソフトウェアで高品質な再生が可能な符号列を、試聴用ファイルと暗号化された高品質化ファイルに分解する信号処理の方法の具体例を示すフローチャートである。先ずS31において、高品質な再生が可能な符号列の、試聴用ファイルとそれを高品質化する高品質化ファイルへの分解を行なう。次にS32において、高品質化ファイルを、殆ど規則的な値をとる符号列部分と、その他の符号列部分に分離する。そして、S33において殆ど規則的な値をとる符号列部分の暗号化を行ない、S34においては、その他の符号列部分の暗号化を行なう。次にS35において、S33でできた、暗号化された殆ど規則的な値をとる符号列部分と、S34でできた暗号化されたその他の符号列部分の統合を行ない、暗号化された高品質化ファイルを作成し、処理を終了する。ただし、S33における暗号化については処理を省略して、S35において、暗号化されていない殆ど規則的な値をとる符号列部分と、暗号化されたその他の符号列部分を統合するようにしても良い。本出願においては、そのようにして統合されたファイルについても暗号化された高品質化ファイルと呼ぶものとする。

【０１０６】

図32は、本発明の方法により、ソフトウェアで、試聴用ファイルと暗号化された高品質化ファイルから高品質再生可能な符号列の作成を行なう方法の具体例を示すフローチャートである。先ずS41において、暗号化された高品質化ファイルから、暗号化された殆ど規則的な値をとる符号列部分と暗号化されたその他の符号列部分を分離する。次にS42において、殆ど規則的な値をとる符号列部分の暗号の復号を行ない、そしてS43において、その他の符号列部分の暗号の復号を行なう。最後にS44において、試聴用ファイル及び、S42で得られた殆ど規則的な値をとる符号列部分、S43で得られたその他の符号列部分から、高品質再生可能な符号列の作成を行ない、処理を終了する。

【０１０７】

ただし、殆ど規則的な値をとる符号列部分に暗号化が施されていない場合には、S41では、殆ど規則的な値をとる符号列部分と暗号化されたその他の符号列部分への分離を行ない、S42の処理は省略され、S44では、試聴用ファイル及び、S41で得られた殆ど規則的な値をとる符号列部分、S43で得られたその他の符号列部分から、高品質再生可能な符号列の作成を行なう。暗号を復号するために必要な鍵の高品質化ファイルのサーバからの受信には、例えば、既に説明したのと同様な方法を用いることができる。

【０１０８】

以上、符号化ユニット数と中域スペクトル係数を高品質化ファイルに符号化して暗号化する方法について述べたが、本発明の方法は、例えば、本発明人等による日本国特許出願2002-160996(本件出願時未公開)で提案されている、一部のフレームにおいて、例えば元の音楽信号となる第一の信号と、例えば「試聴用信号です。」等といったメッセージ信号となる第二の信号を重畳させた信号を符号化し、これから音楽信号だけを購入したい場合には、上記一部のフレームを上記第一の信号だけを符号化した符号列で置き換える方法に対しても、もちろん、適用することが可能である。図33は、上記のように一部のフレームを置き換える符号列を上述の技術を用いて構成した例である。このように、同期信号等、規則的に同じパターンをとる符号や符号化ユニット数のように殆ど規則的に同じ値をとる符号が暗号化された符号列に含まれていると、既に説明を行なったように、この

暗号を解読される可能性が高くなってしまう。

【０１０９】

図34は、上記の事情を鑑み、本発明の方法により、完全に規則的に、あるいは殆ど規則的に同じパターンをとる符号列部分をA領域としてまとめ、その他の符号列を暗号化する符号列部分をまとめたB領域とは分離して、B領域に関してはB領域用の鍵を用いて暗号化を行ない、A領域に関してはB領域とは異なる鍵で暗号化する、または、全く暗号化しないようにするものである。このようにすることによって、B領域は規則性のない符号列を暗号化することになるので、例えば鍵の総当たり法を用いて解読を試みようとしても、何が正解かわからないため、結局、全体としての安全性が高くなる。

【０１１０】

図35は、本発明の別の方法で図33の暗号解読の可能性を低減するもので、符号列を、元の符号列のうち、完全に規則的に、あるいは殆ど規則的に同じパターンをとる符号列部分をまとめたA領域と、元の符号列のうち、完全に規則的に、あるいは殆ど規則的に同じパターンをとる符号列部分をダミーデータで置き換えた符号列部分に分解する。ここで、上記ダミーデータとしては、適当な方法で発生させた乱数を使用するものとする。ここで図35に示す本発明の別の方法では、C領域に関してはC領域用の鍵を用いて暗号化を行ない、A領域に関してはC領域とは異なる鍵で暗号化する、または、全く暗号化しないようにするものである。このようにすることによって、C領域は規則性のない符号列を暗号化することになるので、例えば鍵の総当たり法を用いて解読を試みようとしても、何が正解かわからないため、結局、全体としての安全性が高くなる。

【０１１１】

以上、試聴用ファイルを高品質化ファイルを使用して高品質化する場合の高品質化ファイルの暗号化方法として、本発明の方法を用いる場合について説明を行なったが、本発明の方法は、例えば、音楽符号列のファイル自身を暗号化する場合にも適用することが可能である。即ち、図34、図35について、一部のフレームのデータを置き換える高品質化用ファイルのフォーマットとして説明を行なったが、音楽符号列全体を図34、図35と同様のフォーマットで暗号化をすることがで

きる。その場合にも、やはり、図34のB領域、図35のC領域については、例えば鍵の総当たり法を用いて解読を試みようとしても、何が正解かわからないため、結局、全体としての安全性が高くなる。即ち、例えば、このように暗号化した符号列を記録媒体に記録し、その鍵を販売することでその内容を聞けるようにする場合等に、本発明の方法で、その安全性を高めることが可能である。

【０１１２】

また以上、オーディオ信号を用いた場合を例にとって説明を行なったが、本発明の方法は画像信号に対しても適用することが可能である。即ち、例えば、画像信号をMPEG-1を用いて符号化を行なう場合、ピクチャ層の開始コードは固定された値となっているが、これを含んだ符号列をそのまま暗号化した場合、既に述べたのと同様の理由により、このピクチャ層の開始コードを元に暗号解読が行なわれる可能性があり、本発明の方法が有効となる。

【０１１３】

さらに、本発明の方法は、符号列を記録する場合のみならず、符号列を伝送する場合にも有効であり、これにより、例えば、放送されているオーディオ信号に対して、試聴用信号の符号列を高品質化する符号列の安全性を高めたり、試聴用信号自身の安全性を高めたりすることも可能である。

【０１１４】

なお、本発明の記載にあたっては、異なる鍵で暗号化された符号列のことを含めて、異なる方法で暗号化された符号列と呼ぶことにする。

【０１１５】

【発明の効果】

以上の説明からも明らかなように、本発明の方法を用いることにより、暗号化されたファイルの解読を困難にすることが可能となり、例えば、試聴用オーディオ符号列を高品質化するための高品質化ファイルの安全性を高めることができるようになった。また、例えば、オーディオ符号列自身に対して暗号化をかける際にも、その安全性を高めることが可能になった。

【図面の簡単な説明】

【図 1】本発明に係わる圧縮データの記録再生装置の一具体例としての記録再生

装置の構成例を示すブロック回路図である。

【図 2】本発明に係わる符号化装置の具体例を示すブロック図である。

【図 3】本発明に係わる符号化装置の変換手段の具体例を示すブロック図である。

【図 4】本発明に係わる符号化装置の信号成分符号化手段の具体例を示すブロック図である。

【図 5】本発明に係わる復号装置の具体例を示すブロック図である。

【図 6】本発明に係わる復号装置の逆変換手段の具体例を示すブロック図である。

【図 7】本発明に係わる復号装置の信号成分復号手段の具体例を示すブロック図である。

【図 8】本発明に係わる符号化方法の具体例を説明するための図である。

【図 9】本発明に係わる符号化方法の具体例を説明するための図である。

【図10】本発明に係わる別の符号化方法の具体例を説明するための図である。

【図11】本発明に係わる別の信号成分符号化手段の具体例を示すブロック図である。

【図12】本発明に係わる別の信号成分復号手段の具体例を示すブロック図である。

【図13】本発明に係わる別の符号化方法の具体例を説明するための図である。

【図14】本発明に係わる符号化方法の具体例を説明するための図である。

【図15】本発明に係わる、符号化方法の具体例を説明するための図である。

【図16】本発明に係わる、別の符号化方法の具体例を説明するための図である。

【図17】本発明に係わる再生手段の具体例を示すブロック図である。

【図18】本発明に係わるダミーデータを置き換える情報のフォーマットの具体例を示す図である。

【図19】本発明に係わる記録手段の具体例を示すブロック図である。

【図20】本発明に係わるダミーデータを置き換える情報の別のフォーマットの具体例を示す図である。

【図21】本発明に係わる符号化方法の具体例を示す図である。

【図22】本発明に係わる高品質化のための追加情報の具体例を示す図である。

【図23】本発明に係わる再生手段の具体例を示すブロック図である。

【図24】本発明に係わる記録手段の具体例を示すブロック図である。

【図25】本発明に係わる再生方法の処理の流れの具体例を示すフローチャートである。

【図26】本発明に係わる記録方法の処理の流れの具体例を示すフローチャートである。

【図27】本発明に係わる高品質化のための追加情報の符号列の暗号化の具体例を示す図である。

【図28】本発明による、高品質化のための追加情報の符号列の暗号化の具体例を示す図である。

【図29】本発明による、高品質な再生が可能な符号列を試聴用ファイルと暗号化された高品質化ファイルに分解する信号処理手段の具体例を示す図である。

【図30】本発明による、試聴用ファイルと暗号化された高品質化ファイルから高品質な再生が可能な符号列を生成する信号処理手段の具体例を示す図である。

【図31】本発明による、高品質な再生が可能な符号列を試聴用ファイルと暗号化された高品質化ファイルに分解する信号処理の流れの具体例を示すフローチャートである。

【図32】本発明による、試聴用ファイルと暗号化された高品質化ファイルから高品質な再生が可能な符号列を生成する信号処理の流れの具体例を示すフローチャートである。

【図33】本発明に係わる他の高品質化のための追加情報の符号列、または、再生可能な符号列の暗号化の具体例を示す図である。

【図34】本発明による、他の高品質化のための追加情報の符号列、または、再生可能な符号列の暗号化の具体例を示す図である。

【図35】本発明による、さらに他の高品質化のための追加情報の符号列、または、再生可能な符号列の暗号化の具体例を示す図である。

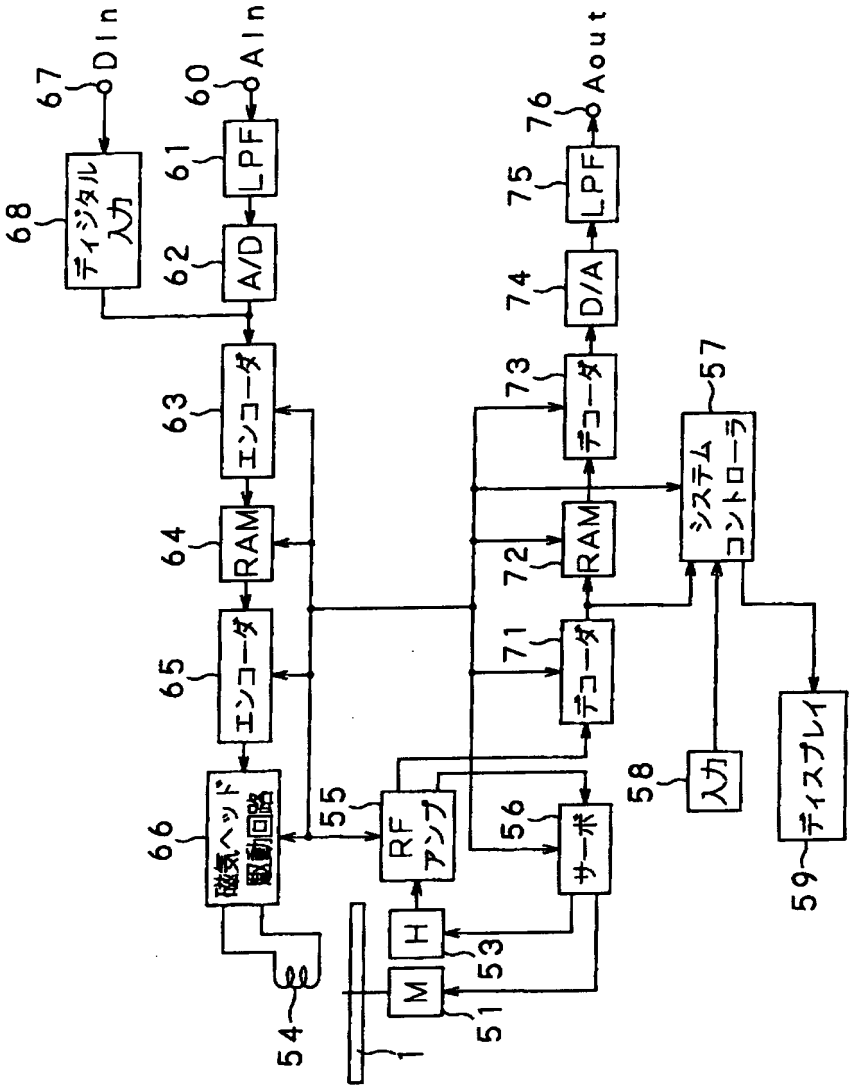
【符号の説明】

１８０１，１８２１，１８４１，１８６１，１８８１　符号列分解手段、　１

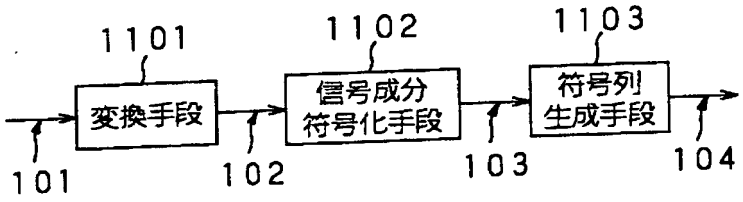
８０２，１８２２　符号列書き換え手段、　１８０３，１８４２　信号成分復号手段、　１８０４，１８４３　逆変換手段、　１８０５，１８２４，１８４４，１８６３，１８８６，１９０５　制御手段、　１８２３，１８６２　記録手段、　１８８２　高品質化データ分離手段、　１８８３，１９０２　暗号化手段Ａ、　１８８４，１９０３　暗号化手段Ｂ、　１８８５　高品質化符号列統合手段、　１９０１　高品質化符号列分離手段、　１９０４　高品質化手段

【書類名】　　図面

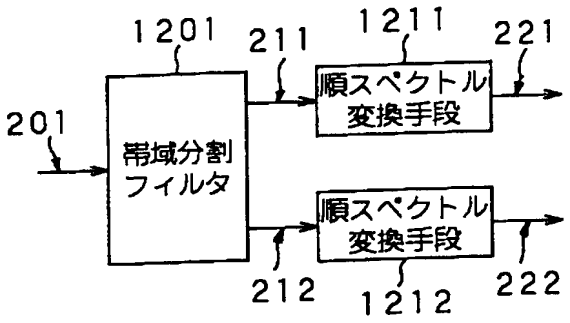
【図１】


Din
Ain
Aout
ディジタル入力
LPF
A/D
エンコーダ
RAM
エンコーダ
磁気ヘッド駆動回路
RF アンプ
H
M
サーボ
デコーダ
RAM
デコーダ
D/A
LPF
システム コントローラ
入力
ディスプレイ
67
60
76
68
61
75
62
74
63
73
57
64
72
65
71
66
55
56
58
59
54
53
51
1

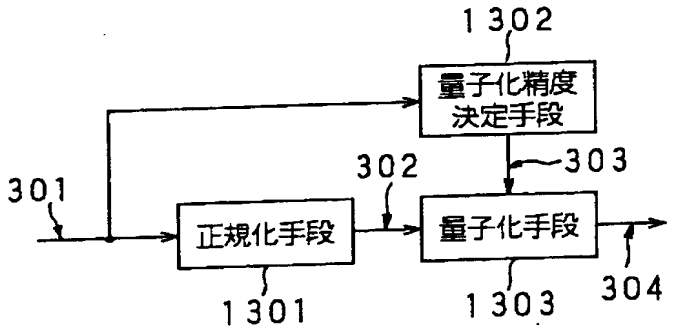
【図２】


1101
1102
1103
変換手段
信号成分 符号化手段
符号列 生成手段
101
102
103
104

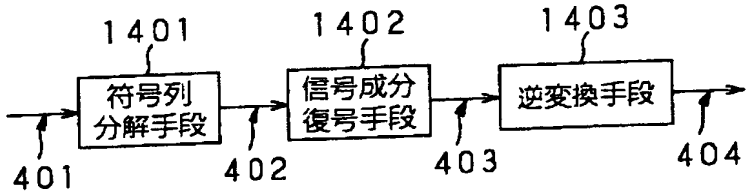
【図３】


1201
211
1211
221
201
帯域分割
フィルタ
順スペクトル
変換手段
順スペクトル
変換手段
212
1212
222

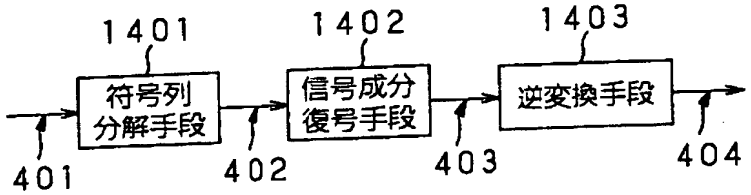
【図４】


1302
量子化精度
決定手段
303
302
301
正規化手段
量子化手段
304
1301
1303

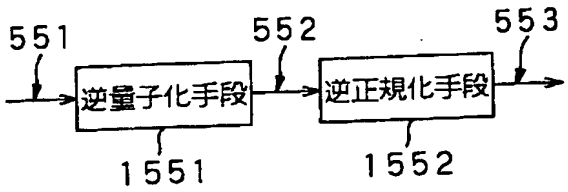
【図５】


1401
1402
1403
符号列
分解手段
信号成分
復号手段
逆変換手段
401
402
403
404

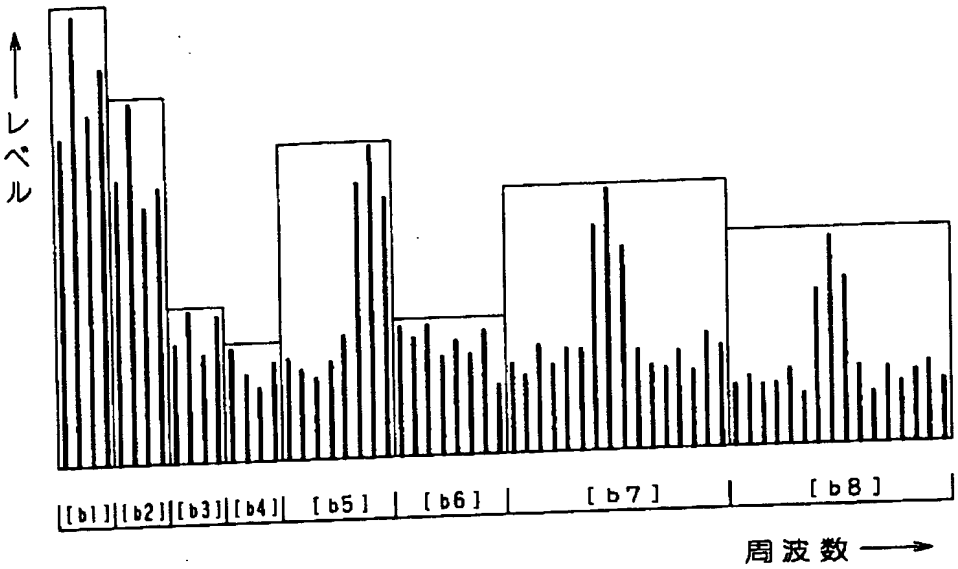
【図６】


1401
1402
1403
符号列
分解手段
信号成分
復号手段
逆変換手段
401
402
403
404

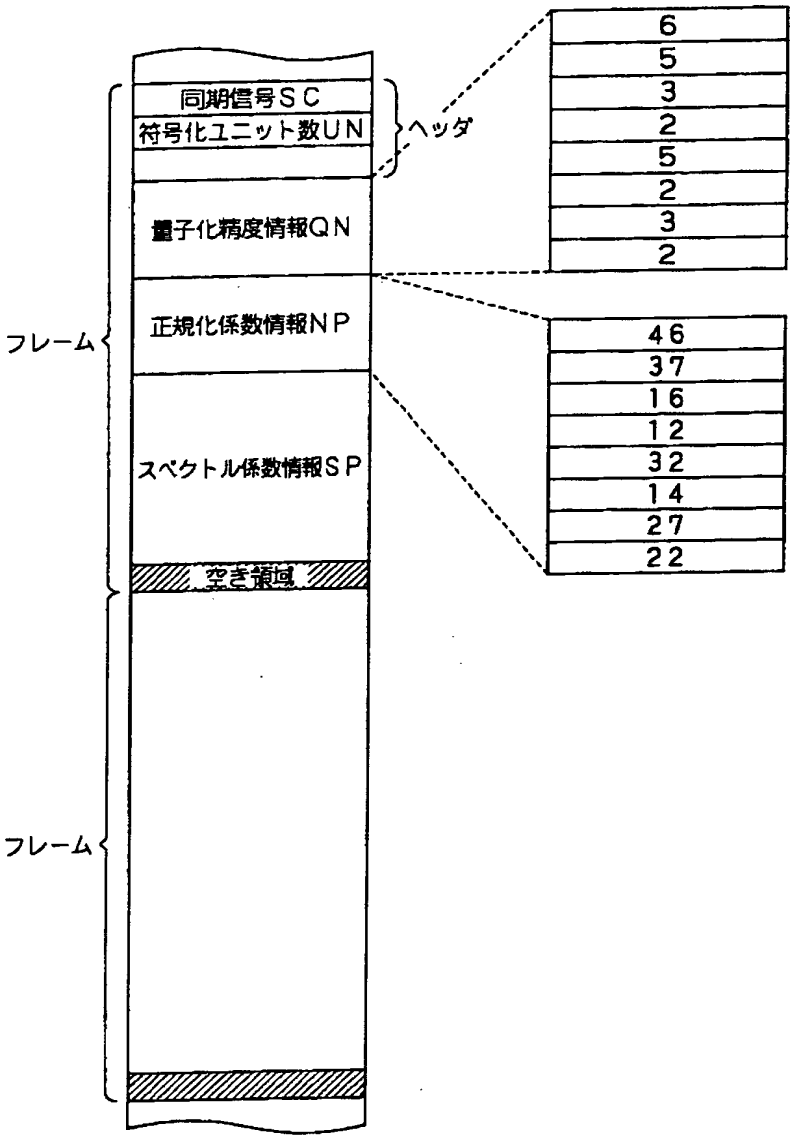
【図７】



【図８】



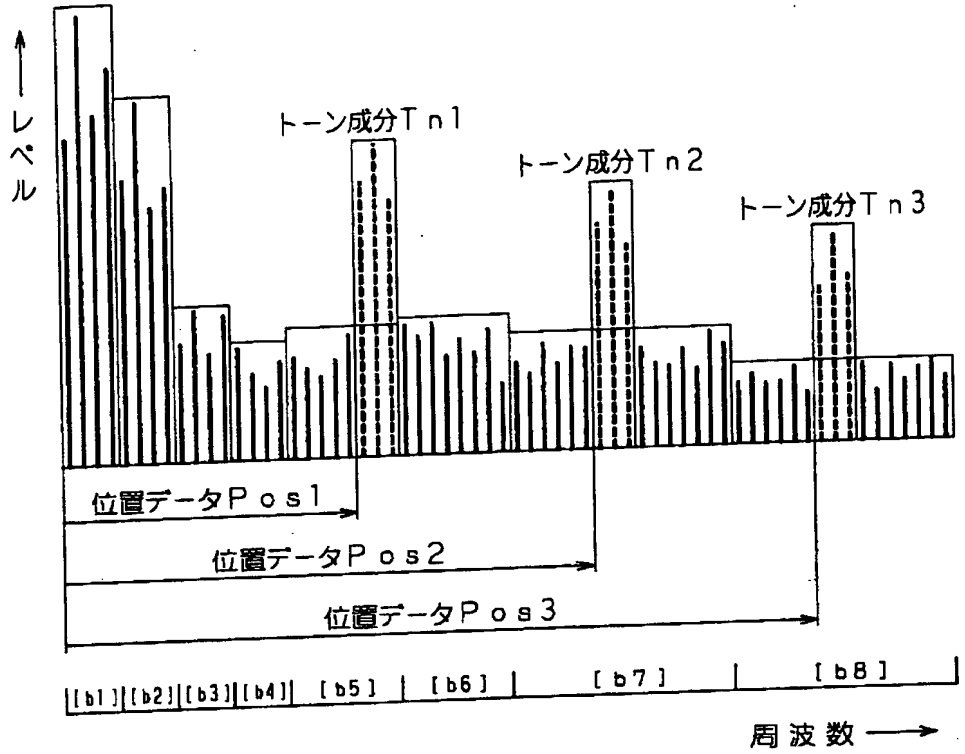
【図９】



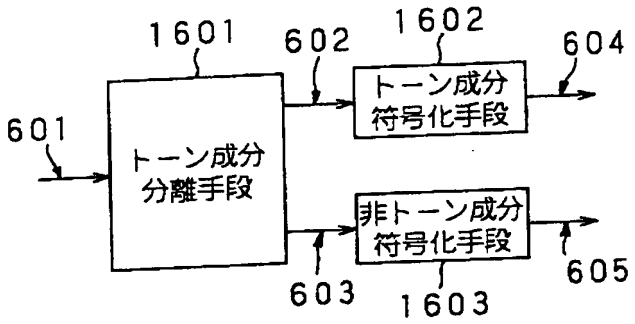



出証特２００３－３０４４９４３

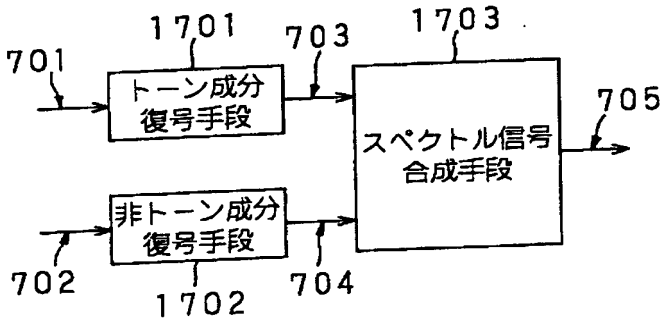
【図１０】


レベル
トーン成分Ｔｎ１
トーン成分Ｔｎ２
トーン成分Ｔｎ３
位置データＰｏｓ１
位置データＰｏｓ２
位置データＰｏｓ３
[b1] [b2] [b3] [b4] [b5] [b6] [b7] [b8]
周波数

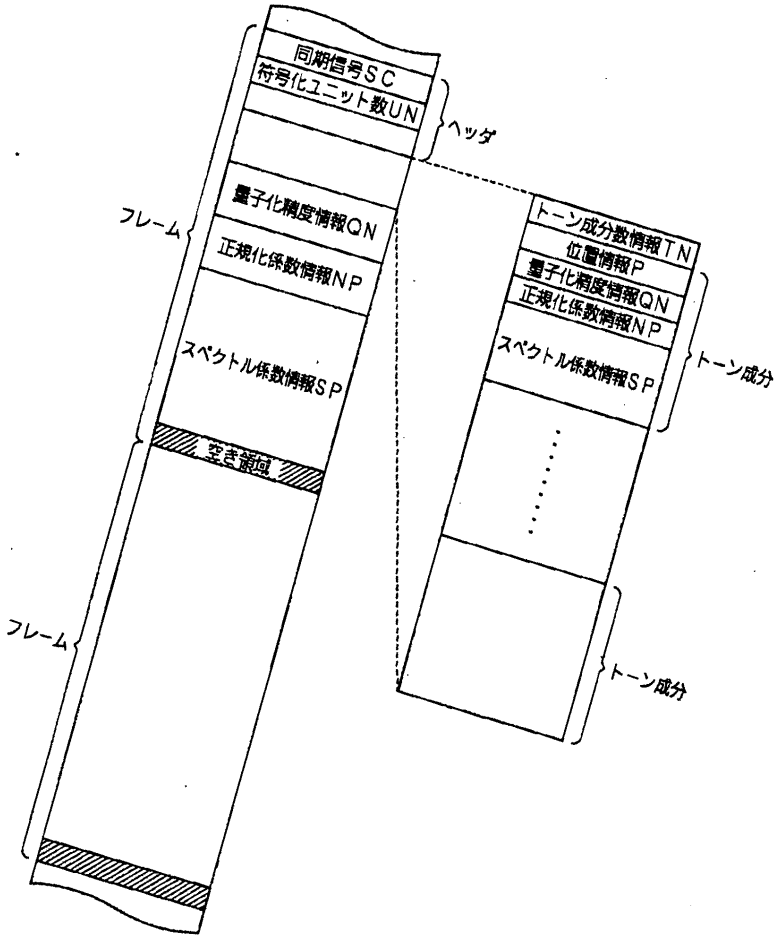
【図１１】


1601
602
1602
604
601
トーン成分
分離手段
トーン成分
符号化手段
非トーン成分
符号化手段
605
603
1603

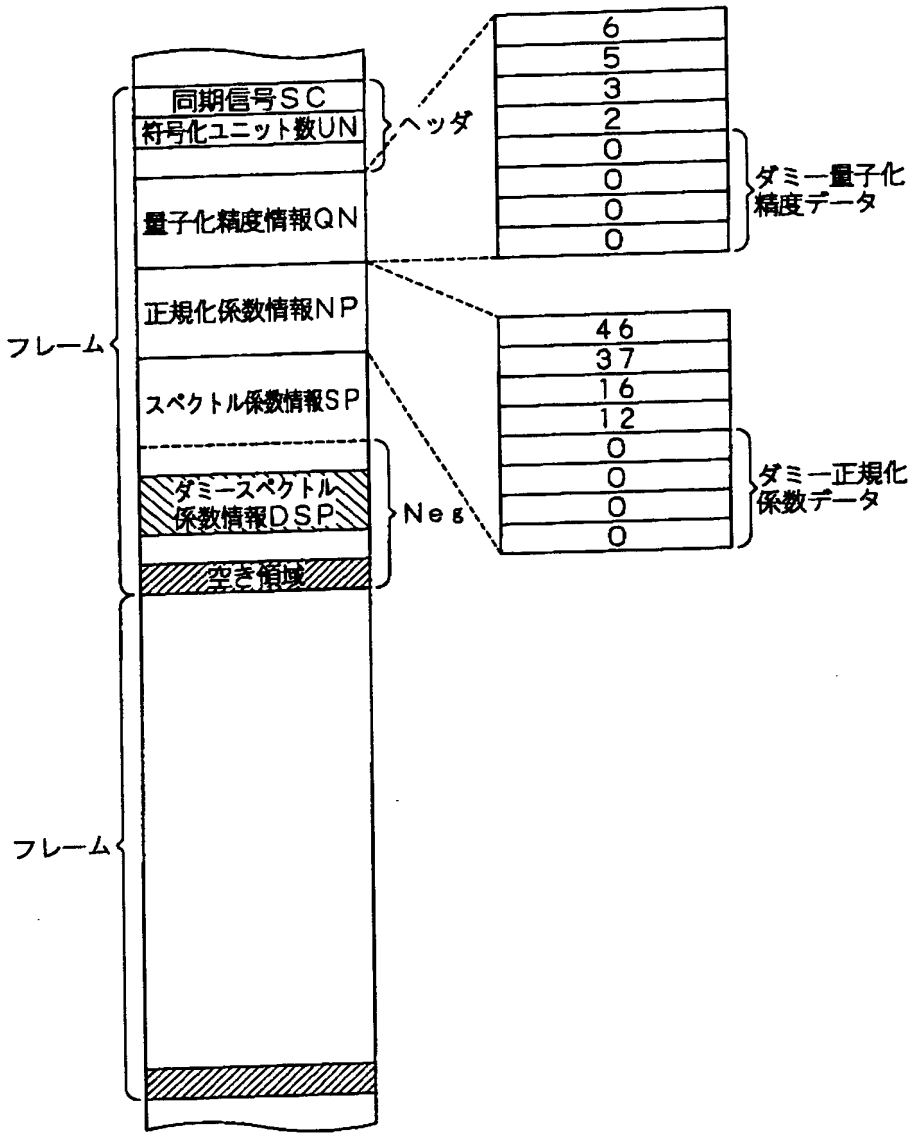
【図１２】


1701
703
1703
701
トーン成分
復号手段
スペクトル信号
合成手段
705
非トーン成分
復号手段
702
704
1702

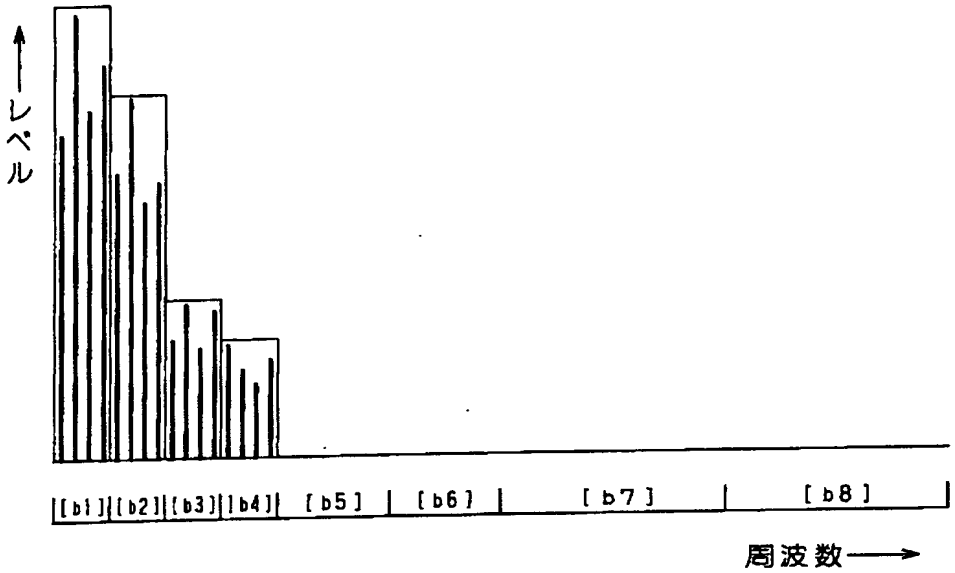
【図１３】


同期信号ＳＣ
符号化ユニット数ＵＮ
ヘッダ
フレーム
量子化精度情報ＱＮ
正規化係数情報ＮＰ
スペクトル係数情報ＳＰ
空き領域
フレーム
トーン成分数情報ＴＮ
位置情報Ｐ
量子化精度情報ＱＮ
正規化係数情報ＮＰ
スペクトル係数情報ＳＰ
トーン成分
トーン成分

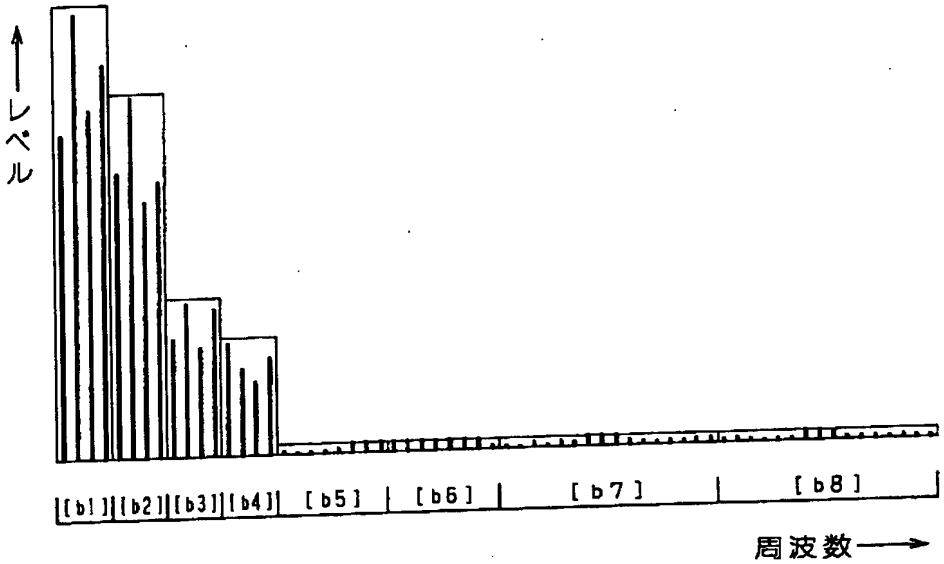
【図１４】


同期信号SC
符号化ユニット数UN
ヘッダ
量子化精度情報QN
正規化係数情報NP
スペクトル係数情報SP
ダミースペクトル係数情報DSP
Neg
空き領域
フレーム
フレーム
6
5
3
2
0
0
0
0
ダミー量子化精度データ
46
37
16
12
0
0
0
0
ダミー正規化係数データ

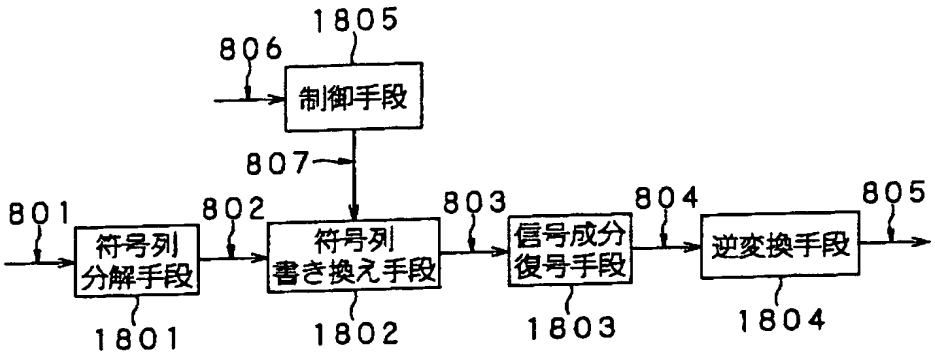
【図１５】



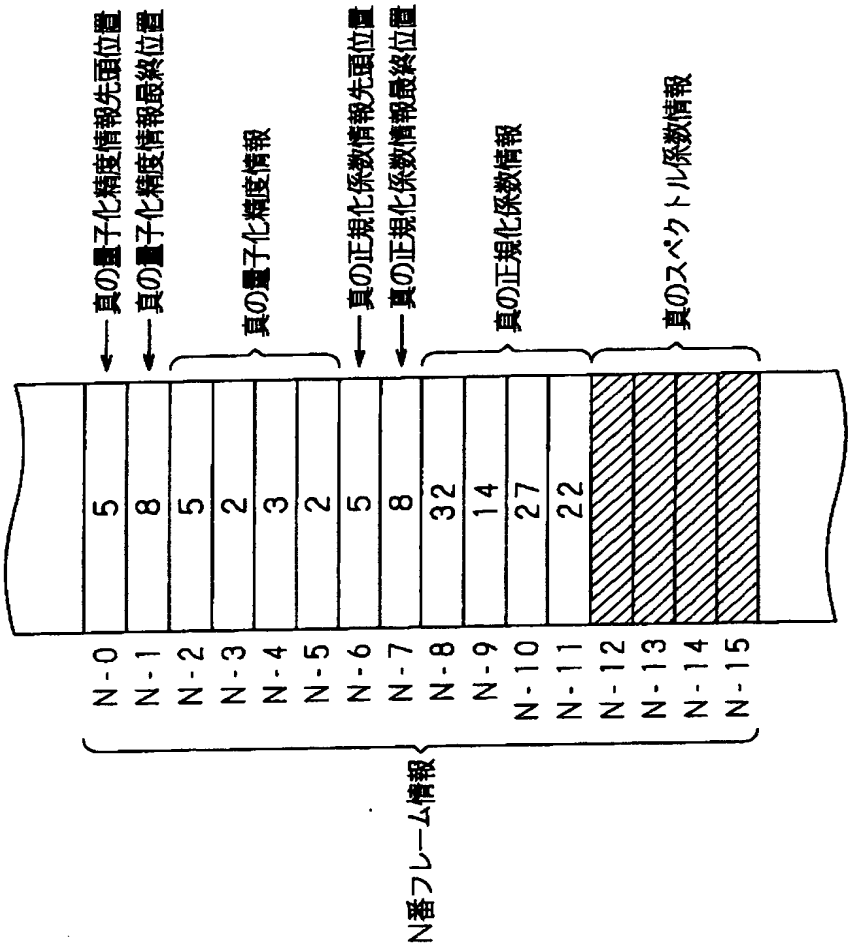
【図１６】



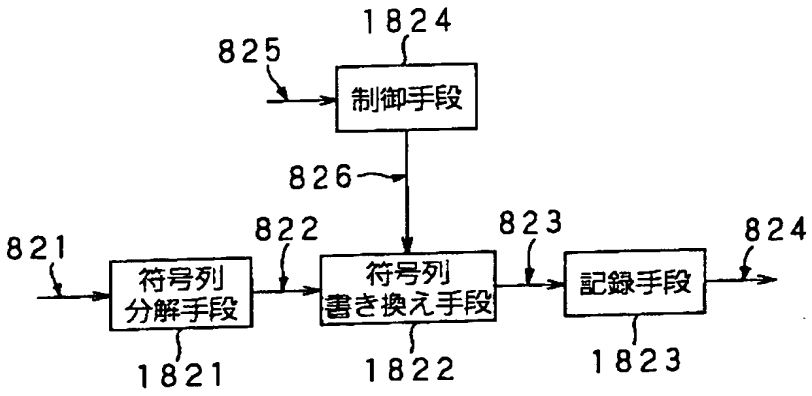
【図１７】


1805
806
制御手段
807
801
802
803
804
805
符号列
分解手段
符号列
書き換え手段
信号成分
復号手段
逆変換手段
1801
1802
1803
1804

【図１８】


真の量子化精度情報先頭位置
真の量子化精度情報最終位置
真の量子化精度情報
真の正規化係数情報先頭位置
真の正規化係数情報最終位置
真の正規化係数情報
真のスペクトル係数情報
5
8
5
2
3
2
5
8
32
14
27
22
N-0
N-1
N-2
N-3
N-4
N-5
N-6
N-7
N-8
N-9
N-10
N-11
N-12
N-13
N-14
N-15
N番フレーム情報

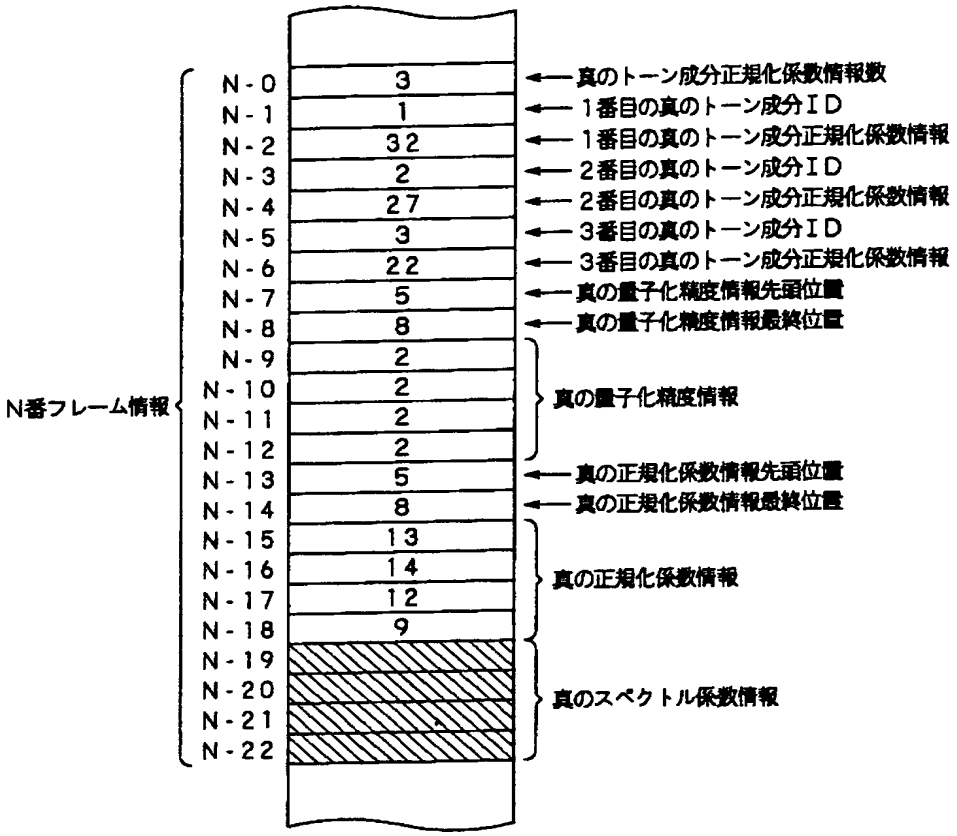
【図１９】



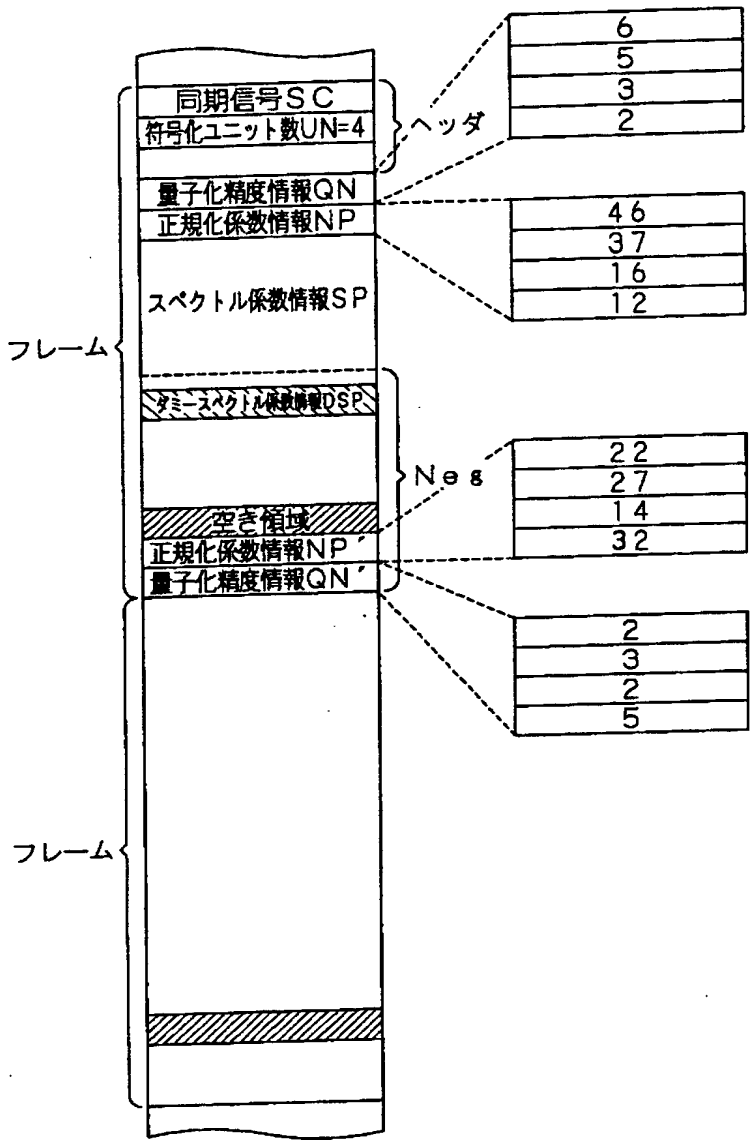



出証特２００３－３０４４９４３

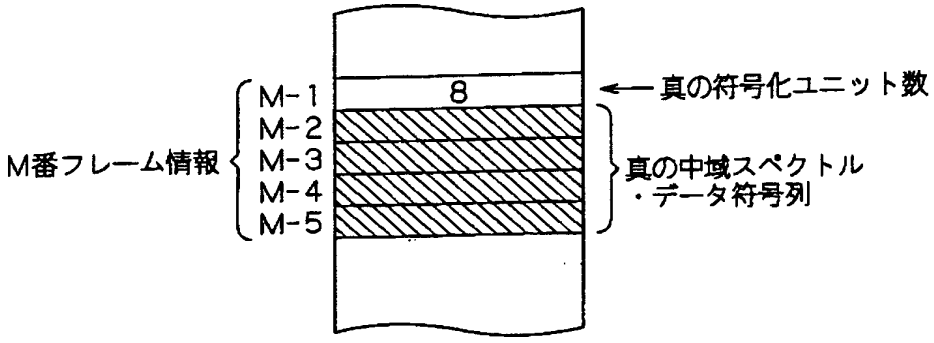
【図２０】


N番フレーム情報
N-0
3
真のトーン成分正規化係数情報数
N-1
1
1番目の真のトーン成分ＩＤ
N-2
32
1番目の真のトーン成分正規化係数情報
N-3
2
2番目の真のトーン成分ＩＤ
N-4
27
2番目の真のトーン成分正規化係数情報
N-5
3
3番目の真のトーン成分ＩＤ
N-6
22
3番目の真のトーン成分正規化係数情報
N-7
5
真の量子化精度情報先頭位置
N-8
8
真の量子化精度情報最終位置
N-9
2
N-10
2
N-11
2
N-12
2
真の量子化精度情報
N-13
5
真の正規化係数情報先頭位置
N-14
8
真の正規化係数情報最終位置
N-15
13
N-16
14
N-17
12
N-18
9
真の正規化係数情報
N-19
N-20
N-21
N-22
真のスペクトル係数情報

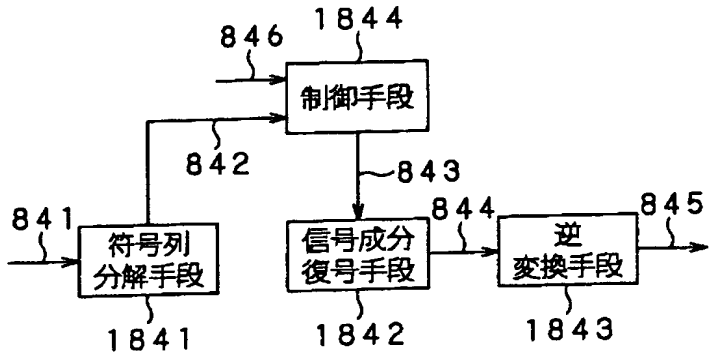
【図２１】


同期信号ＳＣ
符号化ユニット数UN=4
ヘッダ
6
5
3
2
量子化精度情報QN
正規化係数情報NP
スペクトル係数情報SP
46
37
16
12
フレーム
ダミースペクトル係数情報DSP
Neg
空き領域
正規化係数情報NP'
量子化精度情報QN'
22
27
14
32
2
3
2
5
フレーム

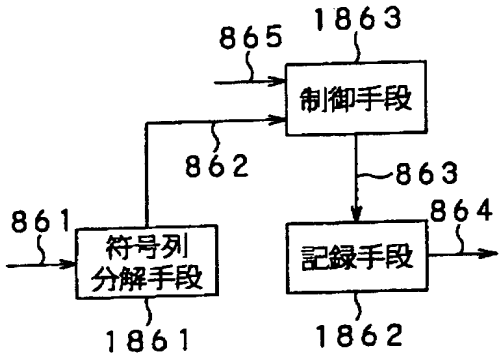
【図２２】


M-1
8
← 真の符号化ユニット数
M-2
M-3
M-4
M-5
M番フレーム情報
真の中域スペクトル
・データ符号列

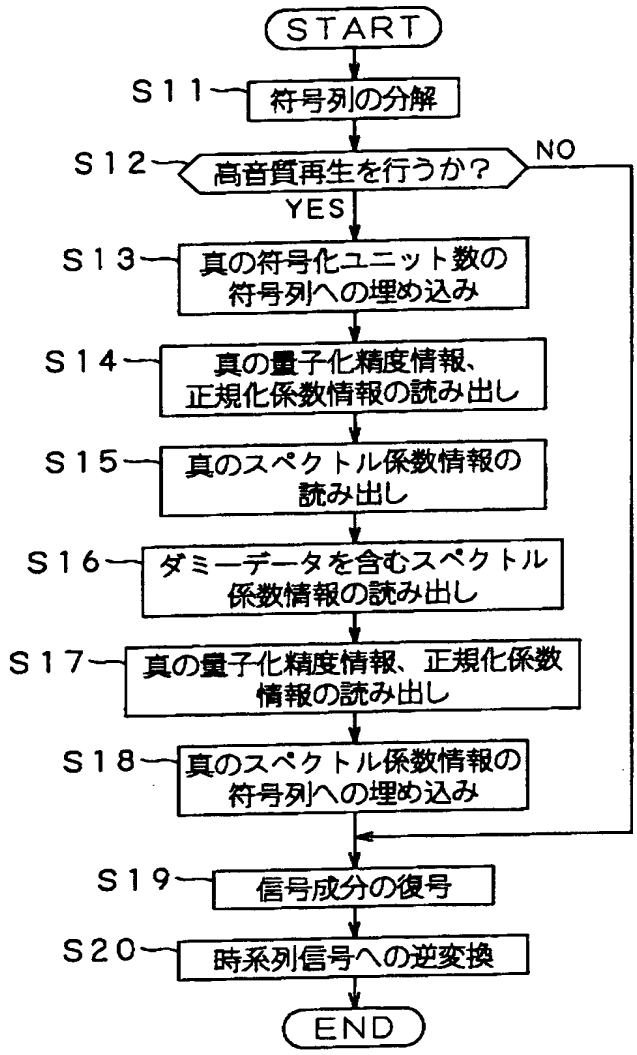
【図２３】


846
1844
制御手段
842
843
841
844
845
符号列
分解手段
信号成分
復号手段
逆
変換手段
1841
1842
1843

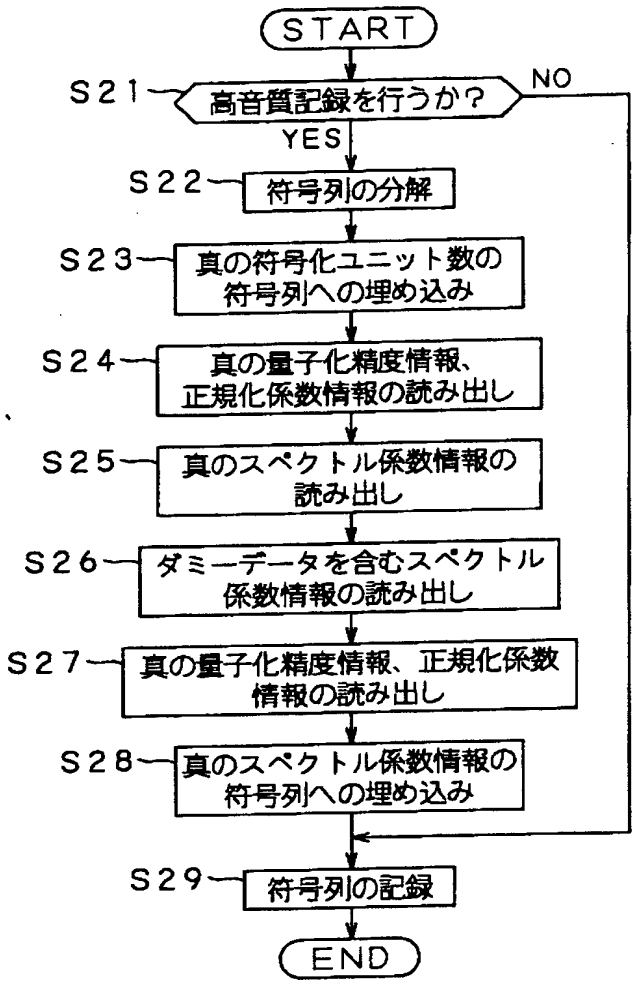
【図２４】


865
1863
制御手段
862
863
861
864
符号列
分解手段
記録手段
1861
1862

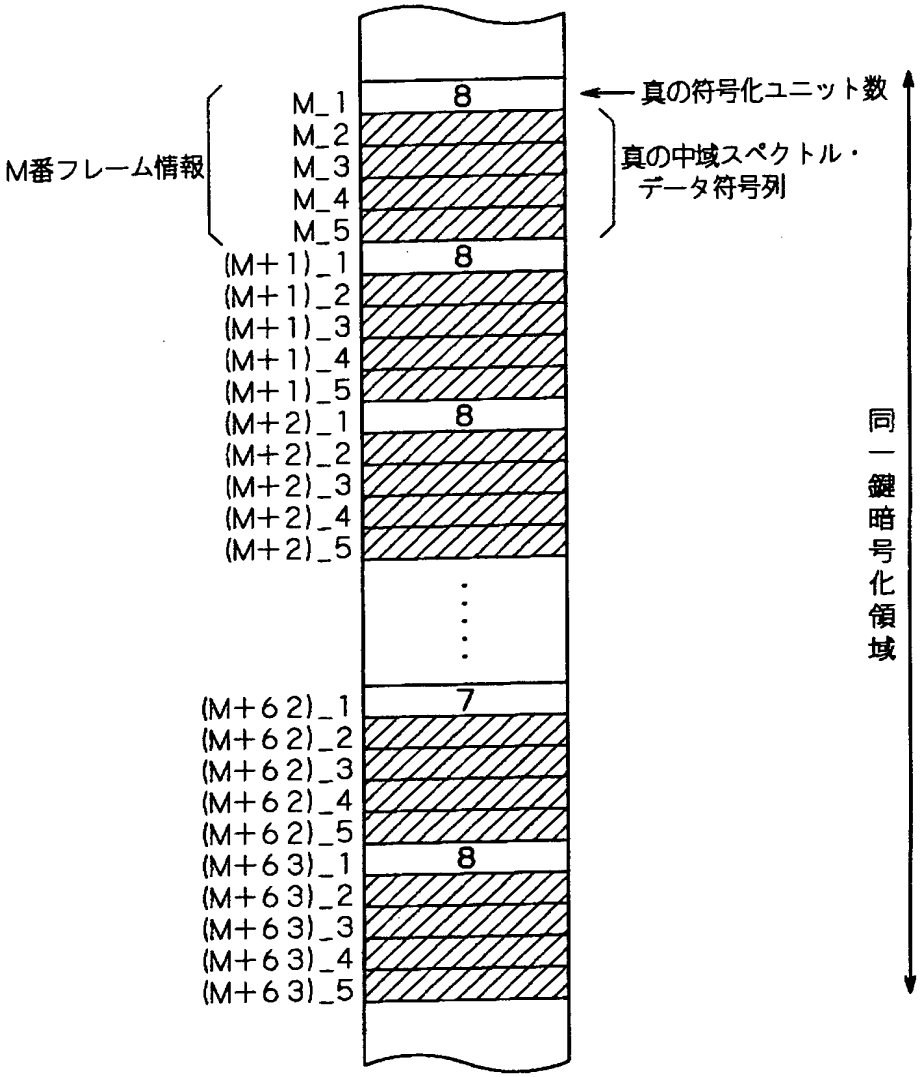
【図２５】


START
S11
符号列の分解
S12
高音質再生を行うか？
NO
YES
S13
真の符号化ユニット数の符号列への埋め込み
S14
真の量子化精度情報、正規化係数情報の読み出し
S15
真のスペクトル係数情報の読み出し
S16
ダミーデータを含むスペクトル係数情報の読み出し
S17
真の量子化精度情報、正規化係数情報の読み出し
S18
真のスペクトル係数情報の符号列への埋め込み
S19
信号成分の復号
S20
時系列信号への逆変換
END

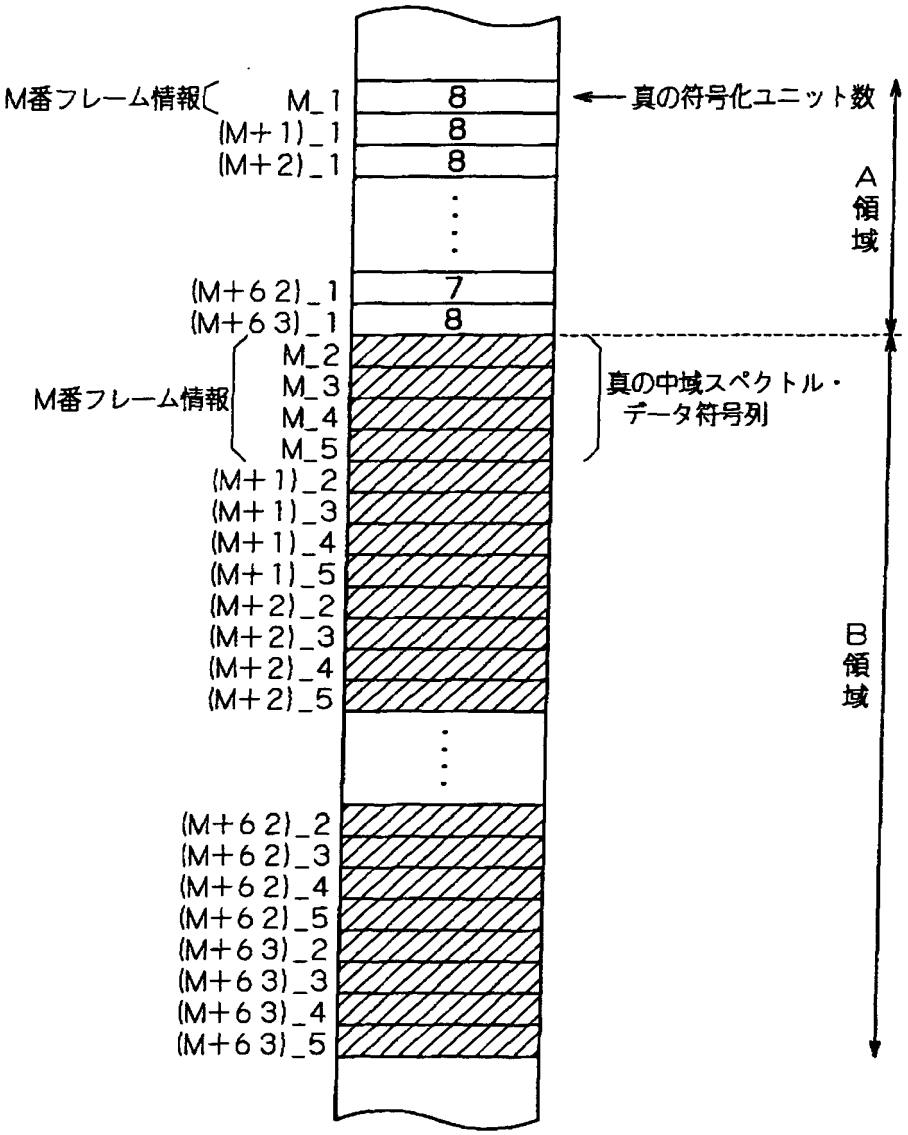
【図２６】


START
S21
高音質記録を行うか？
NO
YES
S22
符号列の分解
S23
真の符号化ユニット数の符号列への埋め込み
S24
真の量子化精度情報、正規化係数情報の読み出し
S25
真のスペクトル係数情報の読み出し
S26
ダミーデータを含むスペクトル係数情報の読み出し
S27
真の量子化精度情報、正規化係数情報の読み出し
S28
真のスペクトル係数情報の符号列への埋め込み
S29
符号列の記録
END

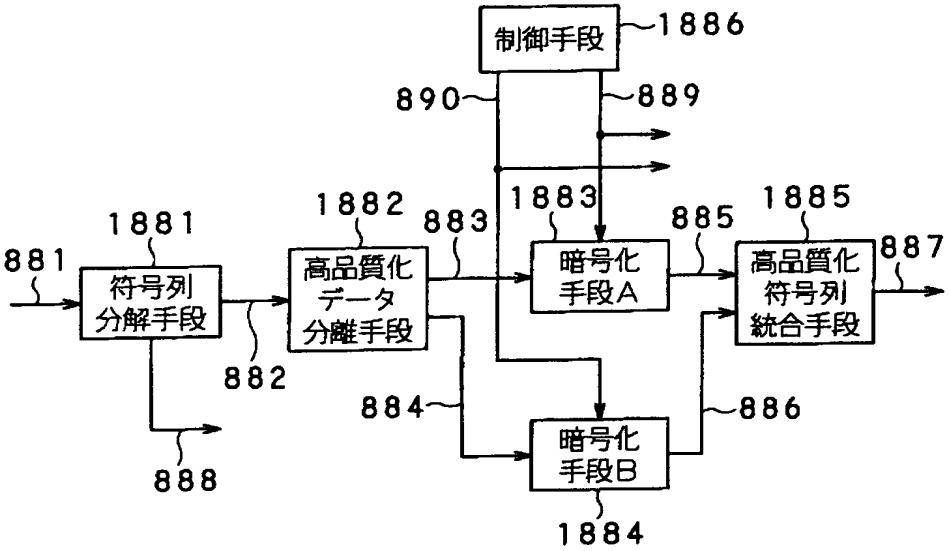
【図２７】


M_1
M_2
M_3
M_4
M_5
(M+1)_1
(M+1)_2
(M+1)_3
(M+1)_4
(M+1)_5
(M+2)_1
(M+2)_2
(M+2)_3
(M+2)_4
(M+2)_5
(M+62)_1
(M+62)_2
(M+62)_3
(M+62)_4
(M+62)_5
(M+63)_1
(M+63)_2
(M+63)_3
(M+63)_4
(M+63)_5
8
8
8
7
8
真の符号化ユニット数
真の中域スペクトル・
データ符号列
M番フレーム情報
同一鍵暗号化領域

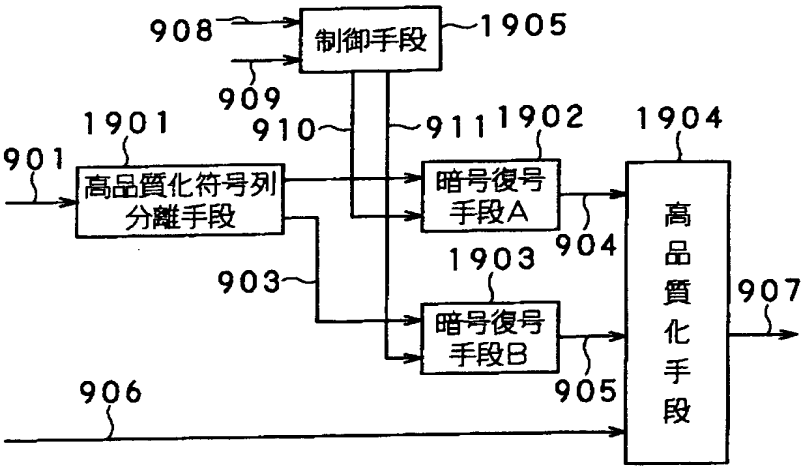
【図２８】


M番フレーム情報
M_1
(M+1)_1
(M+2)_1
(M+62)_1
(M+63)_1
M番フレーム情報
M_2
M_3
M_4
M_5
(M+1)_2
(M+1)_3
(M+1)_4
(M+1)_5
(M+2)_2
(M+2)_3
(M+2)_4
(M+2)_5
(M+62)_2
(M+62)_3
(M+62)_4
(M+62)_5
(M+63)_2
(M+63)_3
(M+63)_4
(M+63)_5
8
8
8
7
8
真の符号化ユニット数
A領域
真の中域スペクトル・データ符号列
B領域

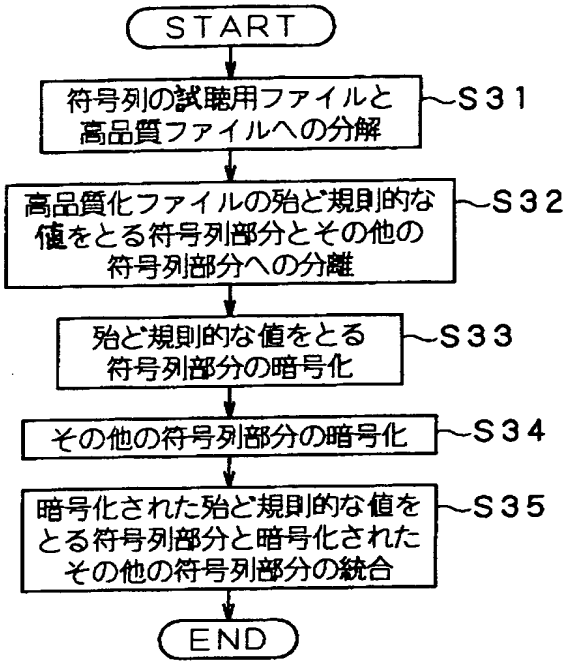
【図２９】


制御手段
1886
890
889
1881
881
符号列
分解手段
1882
883
高品質化
データ
分離手段
1883
暗号化
手段A
885
1885
高品質化
符号列
統合手段
887
882
884
886
888
暗号化
手段B
1884

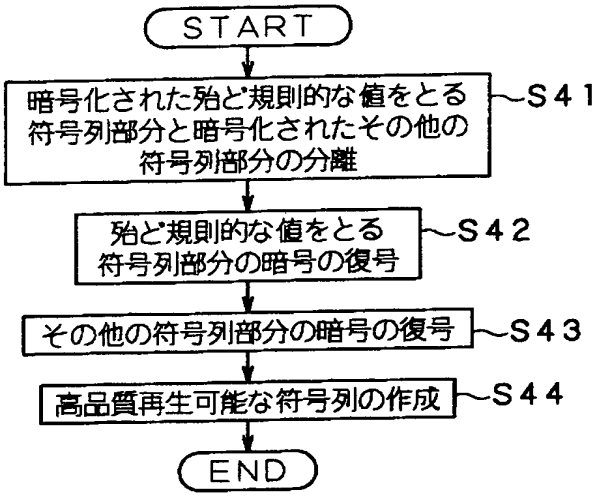
【図３０】


908
制御手段
1905
909
1901
910
911
1902
1904
901
高品質化符号列
分離手段
暗号復号
手段A
904
1903
903
907
暗号復号
手段B
905
高品質化手段
906

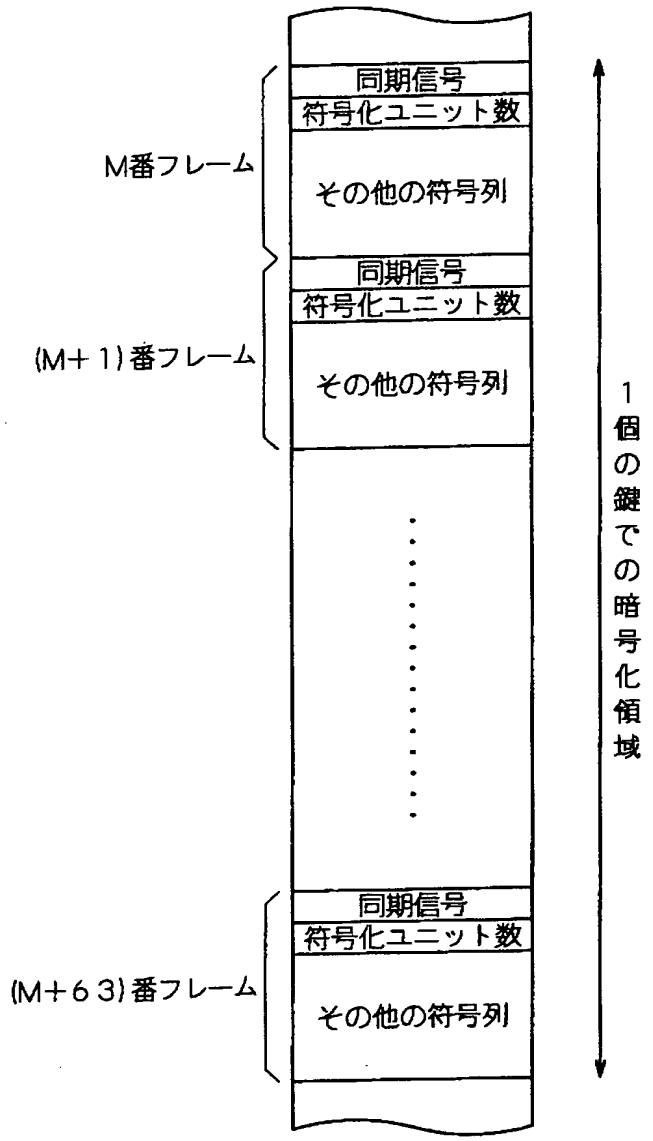
【図３１】


START
符号列の試聴用ファイルと高品質ファイルへの分解
S31
高品質化ファイルの殆ど規則的な値をとる符号列部分とその他の符号列部分への分離
S32
殆ど規則的な値をとる符号列部分の暗号化
S33
その他の符号列部分の暗号化
S34
暗号化された殆ど規則的な値をとる符号列部分と暗号化されたその他の符号列部分の統合
S35
END

【図３２】


START
暗号化された殆ど規則的な値をとる符号列部分と暗号化されたその他の符号列部分の分離
S41
殆ど規則的な値をとる符号列部分の暗号の復号
S42
その他の符号列部分の暗号の復号
S43
高品質再生可能な符号列の作成
S44
END

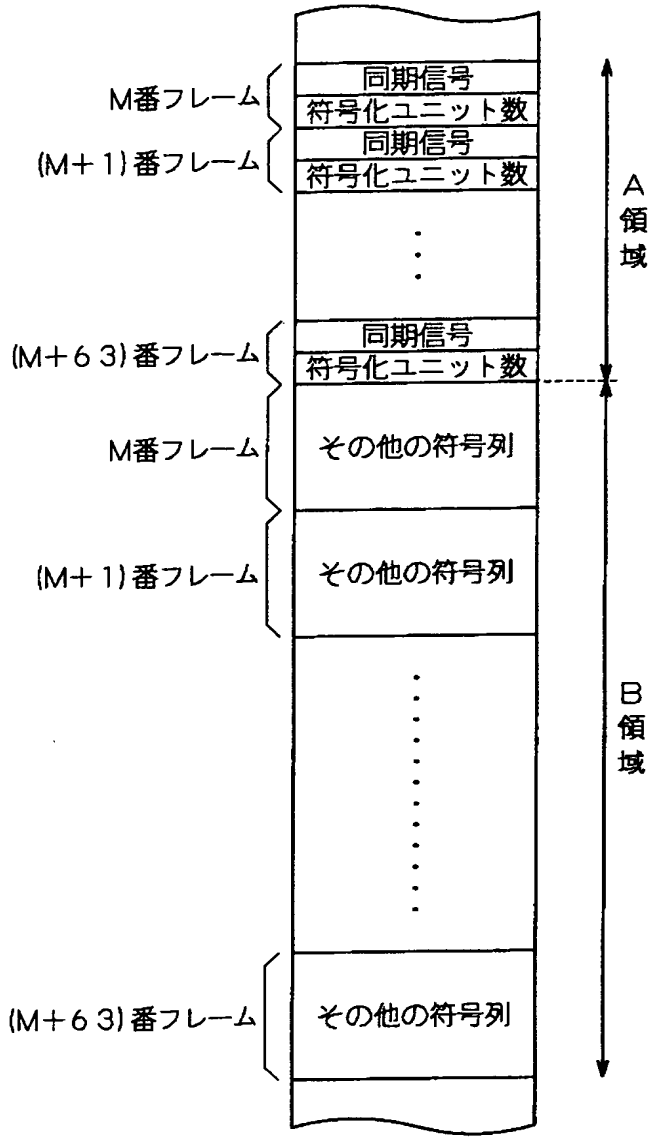
【図３３】



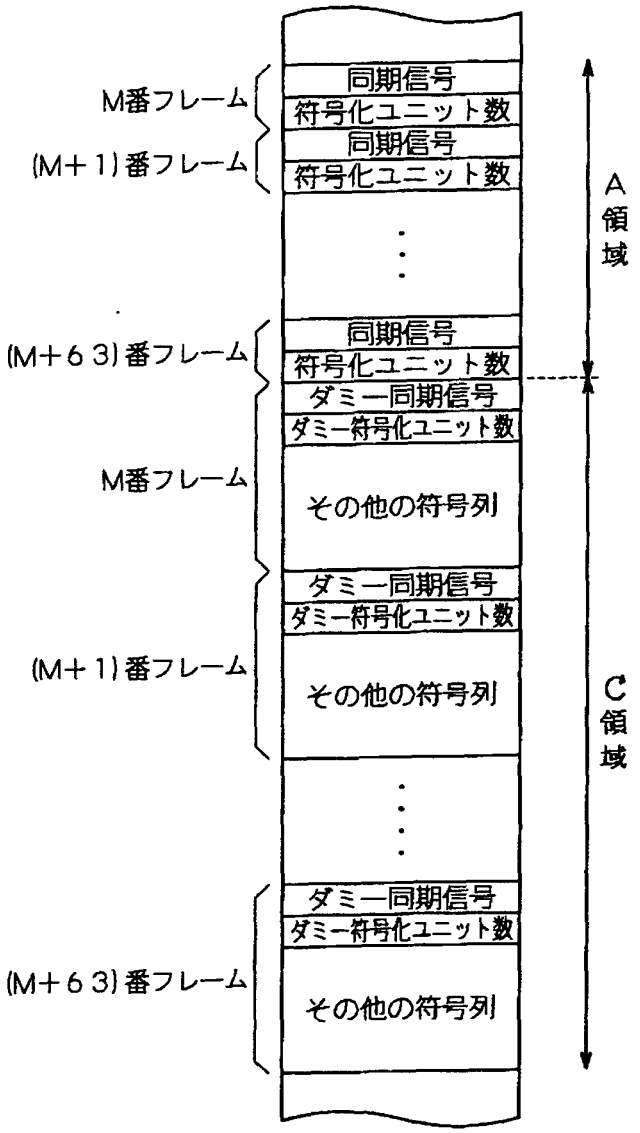



出証特２００３－３０４４９４３

【図３４】


M番フレーム
(M＋1)番フレーム
(M＋63)番フレーム
M番フレーム
(M＋1)番フレーム
(M＋63)番フレーム
同期信号
符号化ユニット数
同期信号
符号化ユニット数
同期信号
符号化ユニット数
その他の符号列
その他の符号列
その他の符号列
A領域
B領域

【図３５】


M番フレーム
(M+1)番フレーム
(M+63)番フレーム
同期信号
符号化ユニット数
ダミー同期信号
ダミー符号化ユニット数
その他の符号列
A領域
C領域

【書類名】　要約書

【要約】

【課題】　試聴用オーディオ符号列を高品質化するための高品質化ファイルの安全性を高める。

【解決手段】　原符号列は、符号列分解手段1881において、試聴用データ881と高品質化データ882に分解される。高品質化データ882は、高品質化データ分離手段1882において、完全に、あるいは殆ど規則性を持つデータ883とそれ以外のデータ884に分離される。データ883は、暗号化しない、あるいは、データ884と別の暗号化処理により暗号化する。これにより、他の重要データの暗号が解読されることを防止するようにする。

【選択図】　図29



出証特２００３－３０４４９４３

# 出　願　人　履　歴　情　報

識別番号　　〔０００００２１８５〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都品川区北品川６丁目７番３５号
氏　名　ソニー株式会社

２．変更年月日　　２００３年　５月１５日
［変更理由］　名称変更
住　所　東京都品川区北品川６丁目７番３５号
氏　名　ソニー株式会社